

11.04.00

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

REC'D 26 APR 2000	
WIPO	PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

1999年 5月24日

出 願 番 号  
Application Number:

平成11年特許願第143988号

出 願 人  
Applicant (s):

ソニー株式会社

EJU

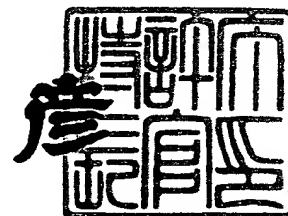
PRIORITY  
DOCUMENT

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 3月10日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3015825

【書類名】 特許願

【整理番号】 9900478304

【提出日】 平成11年 5月24日

【あて先】 特許庁長官 殿

【国際特許分類】 G11B 7/00

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 浅野 智之

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 大澤 義知

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

    【代表者】 出井 伸之

【代理人】

    【識別番号】 100067736

    【弁理士】

    【氏名又は名称】 小池 晃

【選任した代理人】

    【識別番号】 100086335

    【弁理士】

    【氏名又は名称】 田村 榮一

【選任した代理人】

    【識別番号】 100096677

    【弁理士】

    【氏名又は名称】 伊賀 誠司

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第105966号

【出願日】 平成11年 4月13日

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ伝送システム、データ伝送方法、データ送信装置及びデータ受信装置

【特許請求の範囲】

【請求項 1】 伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースと、上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で暗号化して第 1 の伝送モードで上記インターフェースを介して送信し、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで上記インターフェースを介して送信する送信制御手段とを備えるデータ送信装置と、

伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースと、上記インターフェースを介して第 1 の伝送モードで受信される上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で復号し、上記インターフェースを介して第 2 の伝送モードで受信される上記関連データを第 2 の暗号鍵で復号する受信制御手段とを備えるデータ受信装置と

からなることを特徴とするデータ伝送システム。

【請求項 2】 データ伝送に先立って、上記データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行することを特徴とする請求項 1 記載のデータ伝送システム。

【請求項 3】 音楽データを上記第 1 の伝送モードで伝送し、上記音楽データに関する関連データを第 2 の伝送モードで伝送することを特徴とする請求項 1 記載のデータ伝送システム。

【請求項 4】 上記データ送信装置とデータ受信装置を I E E E (The International of Electrical and Electronics Engineers, Inc.) 1 3 9 4 規格に準拠したインターフェースを介して接続し、伝送帯域の保証が必要なデータをアイソクロナス (Isochronous) 伝送モードで伝送し、上記データに関する関連データをアシンクロナス (Asynchronous) 伝送モードで伝送することを特徴とする請求項 1 記載のデータ伝送システム。

【請求項 5】 データ伝送に先立って、上記データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス (Asynchronous) 伝送モードで実行することを特徴とする請求項 4 記載のデータ伝送システム。

【請求項 6】 上記データ受信装置側で  $m$  ビットの 2 つの乱数  $B_{n1}$ ,  $B_{n2}$  を生成してデータ送信装置に送り、

上記データ送信装置側で  $m$  ビットの 2 つの乱数  $A_{n1}$ ,  $A_{n2}$  を生成して上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報  $K_v$  と上記データ受信装置に送った乱数  $A_{n2}$  と受信した乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、その出力の最上位  $m$  ビットをレスポンスデータ  $R_2$  とし、

$$R_2 = H[K_v \parallel A_{n2} \parallel B_{n2}]_{msb\_m}$$

このレスポンスデータ  $R_2$  を上記データ受信装置に送り、

上記データ受信装置は、自分が正当であることを示す情報  $K_v$  と受信した乱数  $A_{n1}$  と上記データ送信装置に送った乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を一方向関数  $H[\ ]$  に入力し、その出力の最上位  $m$  ビットをレスポンスデータ  $R_1$  とし、

$$R_1 = H[K_v \parallel A_{n1} \parallel B_{n1}]_{msb\_m}$$

このレスポンスデータ  $R_1$  を上記データ送信装置に送り、

上記データ送信装置では、自分が正当であることを示す情報  $K_v$  と上記データ受信装置に送った乱数  $A_{n1}$  と受信した乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を一方向関数  $H[\ ]$  に入力し、

$$R'_1 = Hash[K_v \parallel A_{n1} \parallel B_{n1}]_{msb\_m}$$

その出力の最上位  $m$  ビットを参照データ  $R'_1$  とし、この参照データ  $R'_1$  が受信したレスポンスデータ  $R_1$  と一致した場合に、上記連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を一方向関数  $H[\ ]$  に入力し、

$$K_{iso} = H[K_v \parallel A_{n1} \parallel B_{n1}]_{lsb\_m}$$

その出力の最下位  $m$  ビットを Isochronous 伝送で送るデータを暗号化するために使用する暗号鍵  $K_{iso}$  とするとともに、上記連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、

$$K_{async} = H[K_v \parallel A_{n2} \parallel B_{n2}]_{lsb\_m}$$

その出力の最下位  $m$  ビットを Asynchronous 伝送で送るデータを暗号化するために使用する暗号鍵  $K_{async}$  とし、

上記データ受信装置では、自分が正当であることを示す情報  $K_v$  と受信した乱数  $A_{n2}$  と上記データ送信装置に送った乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、

$$R'_2 = H[K_v \parallel A_{n2} \parallel B_{n2}]_{msb\_m}$$

その出力の最上位  $m$  ビットを参照データ  $R'_2$  とし、この参照データ  $R'_2$  が受信したレスポンスデータ  $R_2$  と一致した場合に、上記連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を一方向関数  $H[\ ]$  に入力し、

$$K'_{iso} = H[K_v \parallel A_{n1} \parallel B_{n1}]_{lsb\_m}$$

その出力の最下位  $m$  ビットを Isochronous 伝送で送られてくるデータを復号するために使用する暗号鍵  $K'_{iso}$  とするとともに、上記連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、

$$K'_{async} = H[K_v \parallel A_{n2} \parallel B_{n2}]_{lsb\_m}$$

その出力の最下位  $m$  ビットを Asynchronous 伝送で送られてくるデータを復号するために使用する暗号鍵  $K'_{async}$  とする

ことを特徴とする請求項 5 記載のデータ伝送システム。

【請求項 7】 上記データ受信装置側で  $m$  ビットの 2 つの乱数  $B_{n1}$ ,  $B_{n2}$  を生成してデータ送信装置に送り、

上記データ送信装置側で  $m$  ビットの 2 つの乱数  $A_{n1}$ ,  $A_{n2}$  を生成して上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報  $K_v$  と上記データ受信装置に送った乱数  $A_{n2}$  と受信した乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向

関数  $H[\ ]$  に入力し、

$$R2 = H[Kv \parallel An2 \parallel Bn2]_{msb\_m}$$

その出力の最上位  $m$  ビットをレスポンスデータ  $R2$  とし、このレスポンスデータ  $R2$  を上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報  $Kv$  と上記データ受信装置に送った乱数  $An1$  と受信した乱数  $Bn1$  を連結した連結データ ( $Kv \parallel An1 \parallel Bn1$ ) を生成し、この連結データ ( $Kv \parallel An1 \parallel Bn1$ ) を一方向関数  $H[\ ]$  に入力し、

$$R'1 = H[Kv \parallel An1 \parallel Bn1]_{msb\_p}$$

その出力の最上位  $p$  ビットを参照データ  $R'1$  とするとともに、

$$Kiso = H[Kv \parallel An1 \parallel Bn1]_{lsb\_n}$$

最下位  $n$  ビットを *Isochronous* 伝送で送るデータを暗号化するために使用する暗号鍵  $Kiso$  とし、上記暗号鍵  $Kiso$  と上記データ受信装置に送った乱数  $An1$  と受信した乱数  $Bn1$  を連結した連結データ ( $Kiso \parallel An1 \parallel Bn1$ ) を生成し、この連結データ ( $Kiso \parallel An1 \parallel Bn1$ ) を一方向関数  $H[\ ]$  に入力し、

$$R2 = Hash[Kiso \parallel An1 \parallel Bn1]_{msb\_p}$$

その出力の最上位  $p$  ビットをレスポンスデータ  $R2$  として、このレスポンスデータ  $R2$  を上記データ受信装置に送り、

上記データ受信装置は、自分が正当であることを示す情報  $Kv$  と受信した乱数  $An1$  と上記データ送信装置に送った乱数  $Bn1$  を連結した連結データ ( $Kv \parallel An1 \parallel Bn1$ ) を生成し、この連結データ ( $Kv \parallel An1 \parallel Bn1$ ) を一方向関数  $H[\ ]$  に入力し、

$$R1 = H[Kv \parallel An1 \parallel Bn1]_{msb\_p}$$

その出力の最上位  $p$  ビットをレスポンスデータ  $R1$  とするとともに、

$$K'iso = H[Kv \parallel An1 \parallel Bn1]_{lsb\_n}$$

最下位  $n$  ビットを *Isochronous* 伝送で送られてくるデータを復号するために使用する暗号鍵  $K'iso$  とし、上記暗号鍵  $K'iso$  と受信した乱数  $An2$  と上記データ送信装置に送った乱数  $Bn2$  を連結した連結データ ( $Kv \parallel An2 \parallel Bn2$ ) を生成し、この連結データ ( $Kv \parallel An2 \parallel Bn2$ ) を一方向関数  $H[\ ]$  に入力し、

$$R'2 = H [K'iso \parallel A n 2 \parallel B n 2] msb_p$$

その出力の最上位  $p$  ビットを参照データ  $R'2$  とし、上記データ送信装置から送られてきたレスポンスデータ  $R2$  と上記参照  $R'2$  とを比較して一致した場合に、上記レスポンスデータ  $R1$  を上記データ送信装置に送り、

上記データ送信装置は、上記データ受信装置から送られてきたスポンズデータ  $R1$  と上記参照データ  $R'1$  とを比較して一致した場合に、上記暗号鍵  $Kiso$  と上記データ受信装置に送った乱数  $An2$  と受信した乱数  $Bn2$  を連結した連結データ ( $Kiso \parallel An2 \parallel Bn2$ ) を生成し、この連結データ ( $Kiso \parallel An2 \parallel Bn2$ ) を一方向関数  $H[]$  に入力し、

$$Kasync = H [Kiso \parallel An2 \parallel Bn2] lsb_q$$

その出力の最下位  $q$  ビットを Asynchronous 伝送で送るデータを暗号化するために使用する暗号鍵  $Kasync$  とし、

また、上記データ受信装置は、上記暗号鍵  $K'iso$  と受信した乱数  $An2$  と上記データ送信装置に送った乱数  $Bn2$  を連結した連結データ ( $K'iso \parallel An2 \parallel Bn2$ ) を生成し、この連結データ ( $K'iso \parallel An2 \parallel Bn2$ ) を一方向関数  $H[]$  に入力し、

$$K'async = H [K'iso \parallel An2 \parallel Bn2] lsb_q$$

その出力の最下位  $q$  ビットを Asynchronous 伝送で送られてくるデータを復号するために使用する暗号鍵  $K'async$  とする

ことを特徴とする請求項 5 記載のデータ伝送システム。

【請求項 8】 伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースを介してデータ伝送を行うデータ伝送方法であって、

伝送帯域の保証が必要なデータを第 1 の暗号鍵で暗号化して第 1 の伝送モードで伝送し、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで伝送する

ことを特徴とするデータ伝送方法。

【請求項 9】 データ伝送に先立って、データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する



ことを特徴とする請求項 8 記載のデータ伝送方法。

【請求項 1 0】 音楽データを上記第 1 の伝送モードで伝送し、上記音楽データに関するデータを第 2 の伝送モードで伝送する

ことを特徴とする請求項 8 記載のデータ伝送方法。

【請求項 1 1】 データ送信装置とデータ受信装置との間で、IEEE (The International of Electrical and Electronics Engineers, Inc.) 1 3 9 4 規格に準拠したインターフェースを介して、伝送帯域の保証が必要なデータをアイソクロナス (Isochronous) 伝送モードで伝送し、上記データに関する関連データをアシンクロナス (Asynchronous) 伝送モードで伝送する

ことを特徴とする請求項 7 記載のデータ伝送方法。

【請求項 1 2】 データ伝送に先立って、上記データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス (Asynchronous) 伝送モードで実行する

ことを特徴とする請求項 1 1 記載のデータ伝送方法。

【請求項 1 3】 上記データ受信装置側で  $m$  ビットの 2 つの乱数  $B_{n1}$ ,  $B_{n2}$  を生成してデータ送信装置に送り、

上記データ送信装置側で  $m$  ビットの 2 つの乱数  $A_{n1}$ ,  $A_{n2}$  を生成して上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報  $K_v$  と上記データ受信装置に送った乱数  $A_{n2}$  と受信した乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[]$  に入力し、その出力の最上位  $m$  ビットをレスポンスデータ  $R_2$  とし、

$$R_2 = H [K_v \parallel A_{n2} \parallel B_{n2}]_{msb\_m}$$

このレスポンスデータ  $R_2$  を上記データ受信装置に送り、

上記データ受信装置は、自分が正当であることを示す情報  $K_v$  と受信した乱数  $A_{n1}$  と上記データ送信装置に送った乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) 一方向関数  $H[]$  に入力し、その出力の最上位  $m$  ビットをレスポンスデータ  $R_1$  とし、

$$R_1 = H [K_v \parallel A_{n1} \parallel B_{n1}]_{msb\_m}$$

このレスポンスデータ  $R_1$  を上記データ送信装置に送り、

上記データ送信装置では、自分が正当であることを示す情報  $K_v$  と上記データ受信装置に送った乱数  $A_{n1}$  と受信した乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を一方向関数  $H[\ ]$  に入力し、

$$R'_1 = \text{Hash}[K_v \parallel A_{n1} \parallel B_{n1}]_{\text{msb}_m}$$

その出力の最上位  $m$  ビットを参照データ  $R'_1$  とし、この参照データ  $R'_1$  が受信したレスポンスデータ  $R_1$  と一致した場合に、上記連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を一方向関数  $H[\ ]$  に入力し、

$$K_{\text{iso}} = H[K_v \parallel A_{n1} \parallel B_{n1}]_{\text{lsb}_m}$$

その出力の最下位  $m$  ビットを *Isochronous* 伝送で送るデータを暗号化するために使用する暗号鍵  $K_{\text{iso}}$  とするとともに、上記連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、

$$K_{\text{async}} = H[K_v \parallel A_{n2} \parallel B_{n2}]_{\text{lsb}_m}$$

その出力の最下位  $m$  ビットを *Asynchronous* 伝送で送るデータを暗号化するために使用する暗号鍵  $K_{\text{async}}$  とし、

上記データ受信装置では、自分が正当であることを示す情報  $K_v$  と受信した乱数  $A_{n2}$  と上記データ送信装置に送った乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、

$$R'_2 = H[K_v \parallel A_{n2} \parallel B_{n2}]_{\text{msb}_m}$$

その出力の最上位  $m$  ビットを参照データ  $R'_2$  とし、この参照データ  $R'_2$  が受信したレスポンスデータ  $R_2$  と一致した場合に、上記連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を一方向関数  $H[\ ]$  に入力し、

$$K'_{\text{iso}} = H[K_v \parallel A_{n1} \parallel B_{n1}]_{\text{lsb}_m}$$

その出力の最下位  $m$  ビットを *Isochronous* 伝送で送られてくるデータを復号するために使用する暗号鍵  $K'_{\text{iso}}$  とするとともに、上記連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、

$$K'_{\text{async}} = H[K_v \parallel A_{n2} \parallel B_{n2}]_{\text{lsb}_m}$$

その出力の最下位  $m$  ビットを Asynchronous 伝送で送られてくるデータを復号するために使用する暗号鍵  $K'_{\text{async}}$  とする

ことを特徴とする請求項 12 記載のデータ伝送方法。

【請求項 14】 上記データ受信装置側で  $m$  ビットの 2 つの乱数  $B_{n1}$ ,  $B_{n2}$  を生成してデータ送信装置に送り、

上記データ送信装置側で  $m$  ビットの 2 つの乱数  $A_{n1}$ ,  $A_{n2}$  を生成して上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報  $K_v$  と上記データ受信装置に送った乱数  $A_{n2}$  と受信した乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、

$$R_2 = H[K_v \parallel A_{n2} \parallel B_{n2}]_{\text{msb}_m}$$

その出力の最上位  $m$  ビットをレスポンスデータ  $R_2$  とし、このレスポンスデータ  $R_2$  を上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報  $K_v$  と上記データ受信装置に送った乱数  $A_{n1}$  と受信した乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を一方向関数  $H[\ ]$  に入力し、

$$R'_1 = H[K_v \parallel A_{n1} \parallel B_{n1}]_{\text{msb}_p}$$

その出力の最上位  $p$  ビットを参照データ  $R'_1$  とするとともに、

$$K_{\text{iso}} = H[K_v \parallel A_{n1} \parallel B_{n1}]_{\text{lsb}_n}$$

最下位  $n$  ビットを Isochronous 伝送で送るデータを暗号化するために使用する暗号鍵  $K_{\text{iso}}$  とし、上記暗号鍵  $K_{\text{iso}}$  と上記データ受信装置に送った乱数  $A_{n1}$  と受信した乱数  $B_{n1}$  を連結した連結データ ( $K_{\text{iso}} \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_{\text{iso}} \parallel A_{n1} \parallel B_{n1}$ ) を一方向関数  $H[\ ]$  に入力し、

$$R_2 = \text{Hash}[K_{\text{iso}} \parallel A_{n1} \parallel B_{n1}]_{\text{msb}_p}$$

その出力の最上位  $p$  ビットをレスポンスデータ  $R_2$  として、このレスポンスデータ  $R_2$  を上記データ受信装置に送り、

上記データ受信装置は、自分が正当であることを示す情報  $K_v$  と受信した乱数

$A_{n1}$  と上記データ送信装置に送った乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を一方向関数  $H[\ ]$  に入力し、

$$R_1 = H[K_v \parallel A_{n1} \parallel B_{n1}]_{\text{msb}_p}$$

その出力の最上位  $p$  ビットをレスポンスデータ  $R_1$  とするとともに、

$$K'_{\text{iso}} = H[K_v \parallel A_{n1} \parallel B_{n1}]_{\text{lsb}_n}$$

最下位  $n$  ビットを *Isochronous* 伝送で送られてくるデータを復号するために使用する暗号鍵  $K'_{\text{iso}}$  とし、上記暗号鍵  $K'_{\text{iso}}$  と受信した乱数  $A_{n2}$  と上記データ送信装置に送った乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、

$$R'_2 = H[K'_{\text{iso}} \parallel A_{n2} \parallel B_{n2}]_{\text{msb}_p}$$

その出力の最上位  $p$  ビットを参照データ  $R'_2$  とし、上記データ送信装置から送られてきたレスポンスデータ  $R_2$  と上記参照データ  $R'_2$  とを比較して一致した場合に、上記レスポンスデータ  $R_1$  を上記データ送信装置に送り、

上記データ送信装置は、上記データ受信装置から送られてきたスポンスデータ  $R_1$  と上記参照データ  $R'_1$  とを比較して一致した場合に、上記暗号鍵  $K_{\text{iso}}$  と上記データ受信装置に送った乱数  $A_{n2}$  と受信した乱数  $B_{n2}$  を連結した連結データ ( $K_{\text{iso}} \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_{\text{iso}} \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、

$$K_{\text{async}} = H[K_{\text{iso}} \parallel A_{n2} \parallel B_{n2}]_{\text{lsb}_q}$$

その出力の最下位  $q$  ビットを *Asynchronous* 伝送で送るデータを暗号化するために使用する暗号鍵  $K_{\text{async}}$  とし、

また、上記データ受信装置は、上記暗号鍵  $K'_{\text{iso}}$  と受信した乱数  $A_{n2}$  と上記データ送信装置に送った乱数  $B_{n2}$  を連結した連結データ ( $K'_{\text{iso}} \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K'_{\text{iso}} \parallel A_{n2} \parallel B_{n2}$ ) を一方向関数  $H[\ ]$  に入力し、

$$K'_{\text{async}} = H[K'_{\text{iso}} \parallel A_{n2} \parallel B_{n2}]_{\text{lsb}_q}$$

その出力の最下位  $q$  ビットを *Asynchronous* 伝送で送られてくるデータを復号するために使用する暗号鍵  $K'_{\text{async}}$  とする

ことを特徴とする請求項 12 記載のデータ伝送方法。

【請求項 15】 伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースと、

上記インターフェースを介して、伝送帯域の保証が必要なデータを第 1 の伝送モードで送信し、上記データに関する関連データを第 2 の伝送モードで送信する送信制御手段と

を備えることを特徴とするデータ送信装置。

【請求項 16】 上記送信制御手段は、上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で暗号化して第 1 の伝送モードで上記インターフェースを介して送信し、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで上記インターフェースを介して送信する

ことを特徴とする請求項 15 記載のデータ送信装置。

【請求項 17】 上記送信制御手段は、データ伝送に先立って、データ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する

ことを特徴とする請求項 15 記載のデータ送信装置。

【請求項 18】 上記送信制御手段は、音楽データを上記第 1 の伝送モードで送信し、上記音楽データに関する関連データを第 2 の伝送モードで送信する

ことを特徴とする請求項 15 記載のデータ送信装置。

【請求項 19】 上記インターフェースとして IEEE (The International of Electrical and Electronics Engineers, Inc.) 1394 規格に準拠したインターフェースを有し、

上記送信制御手段は、伝送帯域の保証が必要なデータをアイソクロナス (Isynchronous) 伝送モードで送信し、上記データに関する関連データをアシンクロナス (Asynchronous) 伝送モードで送信する

ことを特徴とする請求項 15 記載のデータ送信装置。

【請求項 20】 上記送信制御手段は、データ伝送に先立って、データ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス (Asynchronous) 伝送モードで実行する

ことを特徴とする請求項 19 記載のデータ送信装置。

【請求項 2 1】 伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースと、

上記インターフェースを介して、伝送帯域の保証が必要なデータを第 1 の伝送モードで受信し、上記データに関する関連データを第 2 の伝送モードで受信する受信制御手段と

を備えることを特徴とするデータ受信装置。

【請求項 2 2】 上記受信制御手段は、上記インターフェースを介して第 1 の伝送モードで受信される上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で復号し、上記インターフェースを介して第 2 の伝送モードで受信される上記関連データを第 2 の暗号鍵で復号する

ことを特徴とする請求項 2 1 記載のデータ受信装置。

【請求項 2 3】 上記受信制御手段は、データ伝送に先立って、データ送信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する

ことを特徴とする請求項 2 1 記載のデータ受信装置。

【請求項 2 4】 上記受信制御手段は、音楽データを上記第 1 の伝送モードで受信し、上記音楽データに関する関連データを第 2 の伝送モードで受信する

ことを特徴とする請求項 2 1 記載のデータ受信装置。

【請求項 2 5】 上記インターフェースとして I E E E (The International of Electrical and Electronics Engineers, Inc.) 1 3 9 4 規格に準拠したインターフェースを有し、

上記受信制御手段は、伝送帯域の保証が必要なデータをアイソクロナス (Isynchronous) 伝送モードで受信し、上記データに関する関連データをアシンクロナス (Asynchronous) 伝送モードで受信する

ことを特徴とする請求項 2 1 記載のデータ受信装置。

【請求項 2 6】 上記受信制御手段は、データ伝送に先立って、データ送信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス (Asynchronous) 伝送モードで実行する

ことを特徴とする請求項 2 5 記載のデータ受信装置。

## 【発明の詳細な説明】

## 【0001】

## 【発明の属する技術分野】

本発明は、データ送信装置からデータ受信装置にデータを一方向に伝送するデータ伝送システム、データ伝送方法、データ送信装置及びデータ受信装置に関する。

## 【0002】

## 【従来の技術】

近年、例えば家庭内において、複数のA V機器をデジタルインターフェースを介して接続し、音楽情報や映像情報などのデジタルデータを伝送したり記録したりするようにしたシステムが普及しつつある。

## 【0003】

例えば、デジタルバスであるIEEE(The International of Electrical and Electronics Engineers,Inc.)1394ハイ・パフォーマンス・シリアル・バス(以下、単にIEEE1394シリアルバスという)のインターフェースを持つビデオカメラやDVDプレーヤなどの機器では、データを高品質で記録することが可能であることから、著作権のあるデータが不正にコピーされてしまうのを防止する必要がある。

## 【0004】

例えば、光磁気ディスク装置に映画情報を記録することが許可されているか否かを表すキーを記憶しておき、このキーを利用して、その光磁気ディスク装置が正当な装置すなわち著作権者からのライセンスを受けた装置であるか否かを認証するようにし、正当な装置として認証された光磁気ディスク装置のみに映画情報の記録を許可するようにすることが行われる。このような場合、映画情報を伝送する側の装置(以下、このような装置をソース(source)という)と、伝送を受けた装置(以下、このような装置をシンク(sink)という)との間で、相手側の装置が適正な装置であるか否かを認証する必要がある。

## 【0005】

このようなシステムにおける著作権保護を目的として、様々な認証方式が提案

されている。これらの認証方式に用いられる認証プロトコルには、暗号アルゴリズムが用いられることが多い。

【 0 0 0 6 】

【発明が解決しようとする課題】

ところで、音楽データを機器間で伝送する際には、例えば、音楽データの伝送途中に伝送が止まったり、伝送できるデータ量が極端に減ったりすると、受信側で音楽の再生に必要なデータが得られなくなり、音楽が途切れてしまう虞があるので、ある程度の帯域を確保した状態で音楽データを伝送する必要がある。

【 0 0 0 7 】

一方、音楽データそのものではないが、音楽データに関連した情報として、例えば歌詞やアーティストの写真などを伝送する場合には、音楽データそのものの伝送する場合に比べて、リアルタイム性を必要としないので、伝送帯域が確保されていない伝送方式を用いて伝送することが可能である。一般に、伝送帯域が確保されていない伝送方式を用いる方が、伝送路全体の帯域を消費しないという点で望まれることが多い。

【 0 0 0 8 】

そこで、本発明の目的は、上述の如き従来の問題点に鑑み、伝送帯域が確保された伝送方式と伝送帯域が確保されていない伝送方式の2種類の伝送方式を採用して、データを確実に伝送することができるようにしたデータ伝送システム、データ伝送方法、データ送信装置及びデータ受信装置を提供することにある。

【 0 0 0 9 】

また、本発明の他の目的は、伝送帯域の保証が必要なデータと上記データに関する関連データを異なる暗号鍵により暗号化して安全に伝送することができるようにしたデータ伝送システム、データ伝送方法、データ送信装置及びデータ受信装置を提供することにある。

【 0 0 1 0 】

さらに、本発明の他の目的は、データ送信装置とデータ受信装置が互いの正当性を認証するとともに、暗号鍵を共有することができるようにしたデータ伝送システム、データ伝送方法、データ送信装置及びデータ受信装置を提供することに



ある。

【0011】

【課題を解決するための手段】

本発明に係るデータ伝送システムは、伝送帯域が保証された第1の伝送モードと伝送帯域が保証されていない第2の伝送モードを持つインターフェースと、上記インターフェースを介して、伝送帯域の保証が必要なデータを第1の伝送モードで送信し、上記データに関する関連データを第2の伝送モードで送信する送信制御手段とを備えるデータ送信装置と、伝送帯域が保証された第1の伝送モードと伝送帯域が保証されていない第2の伝送モードを持つインターフェースと、上記インターフェースを介して、伝送帯域の保証が必要なデータを第1の伝送モードで受信し、上記データに関する関連データを第2の伝送モードで受信する受信制御手段とを備えるデータ受信装置とからなることを特徴とする。

【0012】

本発明に係るデータ伝送方法は、伝送帯域が保証された第1の伝送モードと伝送帯域が保証されていない第2の伝送モードを持つインターフェースを介してデータ伝送を行うデータ伝送方法であって、伝送帯域の保証が必要なデータを第1の伝送モードで伝送し、上記データに関する関連データを第2の伝送モードで伝送することを特徴とする。

【0013】

本発明に係るデータ送信装置は、伝送帯域が保証された第1の伝送モードと伝送帯域が保証されていない第2の伝送モードを持つインターフェースと、上記インターフェースを介して、伝送帯域の保証が必要なデータを第1の伝送モードで送信し、上記データに関する関連データを第2の伝送モードで送信する送信制御手段とを備えることを特徴とする。

【0014】

本発明に係るデータ受信装置は、伝送帯域が保証された第1の伝送モードと伝送帯域が保証されていない第2の伝送モードを持つインターフェースと、上記インターフェースを介して、伝送帯域の保証が必要なデータを第1の伝送モードで受信し、上記データに関する関連データを第2の伝送モードで受信する受信制御

手段とを備えることを特徴とする。

【 0 0 1 5 】

本発明では、伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースを介して、伝送帯域の保証が必要なデータを第 1 の伝送モードで伝送し、上記データに関する関連データを第 2 の伝送モードで伝送する。

【 0 0 1 6 】

上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で暗号化して第 1 の伝送モードで伝送し、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで伝送することができる。また、データ伝送に先立って、データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行することができる。上記第 1 の伝送モードでは音楽データを伝送し、上記第 2 の伝送モードでは上記音楽データに関するデータを第 2 の伝送モードで伝送する。

【 0 0 1 7 】

データ送信装置とデータ受信装置との間のインターフェースとして、例えば I E E E (The International of Electrical and Electronics Engineers, Inc.) 1 3 9 4 規格に準拠したインターフェースを採用することにより、伝送帯域の保証が必要なデータをアイソクロナス (Isynchronous) 伝送モードで伝送し、上記データに関する関連データをアシンクロナス (Asynchronous) 伝送モードで伝送することができる。また、データ伝送に先立って、上記データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス (Asynchronous) 伝送モードで実行することができる。

【 0 0 1 8 】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照しながら説明する。

【 0 0 1 9 】

本発明は、各種デジタル A V (Audio Visual) 機器やパーソナルコンピュータ装置等の電子機器を、例えば I E E E (Institute of Electrical Engineers) 1 3

94バスを介して相互に接続することで、機器間でデータを送受信できるようにしたデータ伝送システム(AVシステム)に適用される。このAVシステムは、デジタル衛星放送を受信して、受信データをダウンロード可能な構成が採られるものである。

#### 【0020】

このAVシステムを含むデジタル衛星放送システムの全体構成を図1に示してある。

#### 【0021】

この図1に示したデジタル衛星放送システムにおいて、デジタル衛星放送の地上局101には、テレビ番組素材サーバ106からのテレビ番組放送のための素材と、楽曲素材サーバ107からの楽曲データの素材と、音声付加情報サーバ108からの音声付加情報と、GUI(Graphical User Interface)データサーバ109からのGUIデータとが送られる。

#### 【0022】

テレビ番組素材サーバ106は、通常の放送番組の素材を提供するサーバである。このテレビ番組素材サーバから送られてくる音楽放送の素材は、動画及び音声とされる。例えば、音楽放送番組であれば、上記テレビ番組素材サーバ106の動画及び音声の素材を利用して、例えば新曲のプロモーション用の動画及び音声が発送されたりすることになる。

#### 【0023】

楽曲素材サーバ107は、オーディオチャンネルを使用して、オーディオ番組を提供するサーバである。このオーディオ番組の素材は音声のみとなる。この楽曲素材サーバ107は、複数のオーディオチャンネルのオーディオ番組の素材を地上局101に伝送する。

#### 【0024】

各オーディオチャンネルの番組放送ではそれぞれ同一の楽曲が所定の単位時間繰り返して放送される。各オーディオチャンネルは、それぞれ、独立しており、その利用方法としては各種考えられる。例えば、1つのオーディオチャンネルでは最新の日本のポップスの数曲を或る一定時間繰り返し放送し、他のオーディオ

チャンネルでは最新の外国のポップスの数曲を或る一定時間繰り返し放送するというようにされる。

【 0 0 2 5 】

音声付加情報サーバ 1 0 8 は、楽曲素材サーバ 1 0 7 から出力される楽曲の時間情報等を提供するサーバである。

【 0 0 2 6 】

G U I データサーバ 1 0 9 は、ユーザが操作に用いる G U I 画面を形成するための「G U I データ」を提供する。例えば後述するような楽曲のダウンロードに関する G U I 画面であれば、配信される楽曲のリストページや各楽曲の情報ページを形成するための画像データ、テキストデータ、アルバムジャケットの静止画を形成するためのデータなどを提供する。更には、A V システム 1 0 3 側にていわゆる E P G (Electrical Program Guide) といわれる番組表表示を行うのに利用される E P G データもここから提供される。

【 0 0 2 7 】

なお、「G U I データ」としては、例えば M H E G (Multimedia Hypermedia Information Coding Experts Group) 方式が採用される。M H E G とは、マルチメディア情報、手順、操作などのそれぞれと、その組み合わせをオブジェクトとして捉え、それらのオブジェクトを符号化したうえで、タイトル（例えば G U I 画面）として制作するためのシナリオ記述の国際標準とされる。また、このデジタル衛星放送システムでは M H E G - 5 を採用するものとする。

【 0 0 2 8 】

地上局 1 0 1 は上記テレビ番組素材サーバ 1 0 6、楽曲素材サーバ 1 0 7、音声付加情報サーバ 1 0 8 及び G U I データサーバ 1 0 9 から伝送された情報を多重化して送信する。

【 0 0 2 9 】

このデジタル衛星放送システムでは、テレビ番組素材サーバ 1 0 6 から伝送されたビデオデータは M P E G (Moving Picture Experts Group) 2 方式により圧縮符号化され、オーディオデータは M P E G 2 オーディオ方式により圧縮符号化される。また、楽曲素材サーバ 1 0 7 から伝送されたオーディオデータは、オーデ

イオチャンネルごとに対応して、例えばMPEG2オーディオ方式と、ATRA C(Adaptive Transform Acoustic Coding)方式の何れか一方の方式により圧縮符号化される。

【0030】

また、これらのデータは多重化の際、キー情報サーバ110からのキー情報を利用して暗号化される。

【0031】

地上局101からの信号は衛星102を介して各家庭の受信設備（以降、AVシステムともいう）103で受信される。衛星102には複数のトランスポンダが搭載されている。1つのトランスポンダは例えば30Mbpsの伝送能力を有している。各家庭のAVシステム103は、パラボラアンテナ111に接続されたIRD(Integrated Receiver Decoder)112と、このIRD112に接続されたモニタ装置114及びMDレコーダ/プレーヤ1とからなる。また、このAVシステム103は、IRD112に対して操作を行うためのリモートコントローラ64と、MDレコーダ/プレーヤ1に対して操作を行うためのリモートコントローラ32を備えている。

【0032】

このAVシステム103では、パラボラアンテナ111で衛星102を介して放送されてきた信号が受信される。この受信信号がパラボラアンテナ111に取り付けられたLNB(Low Noise Block Down Converter)115で所定の周波数に変換され、IRD112に供給される。

【0033】

IRD112における概略的な動作としては、受信信号から所定のチャンネルの信号を選局し、その選局された信号から番組としてのビデオデータ及びオーディオデータの復調を行ってビデオ信号、オーディオ信号として出力する。また、IRD112では、番組としてのデータと共に多重化されて送信されてくる、GUIデータに基づいてGUI画面としての出力も行う。このようなIRD112の出力は、例えばモニタ装置114に対して供給される。これにより、モニタ装置114では、IRD112により受信選局した番組の画像表示及び音声出力が

行われ、また、ユーザの操作に従ってGUI画面を表示させることが可能となる。

#### 【0034】

MDレコーダ/プレーヤ1は、装填されたミニディスクに対するオーディオデータの記録/再生が可能な記録再生装置である。また、このMDレコーダ/プレーヤ1は、オーディオデータ（楽曲データ）及びこれに付随して関連付けされたアルバムジャケット等の静止画像データ（ピクチャファイル）、歌詞やライナーノーツ等のテキストデータ（テキストファイル）をディスクに記録し、かつ、記録されたこれらのピクチャファイル及びテキストファイル等のデータをオーディオデータの再生時間に同期させて再生出力することができるものである。

#### 【0035】

なお、上記オーディオデータに付随したピクチャファイル及びテキストファイル等のデータについては、後述するMDレコーダ/プレーヤ1での扱いに従って、便宜上「AUXデータ」ともいう。

#### 【0036】

ここで、このAVシステム103において、IRD112及びMDレコーダ/プレーヤ1は、IEEE1394バス116によって相互接続されているものとされる。

#### 【0037】

つまり、AVシステム103を構築しているIRD112及びMDレコーダ/プレーヤ1は、それぞれデータ伝送規格としてIEEE1394に対応したデータインターフェイスを備えている。

#### 【0038】

これによって、このAVシステムでは、IRD112にて受信された楽曲としてのオーディオデータ（ダウンロードデータ）を、ATRAC方式により圧縮処理が施されたままの状態ですべて直接取り込んで記録することができる。また、上記オーディオデータと共に送信側からアップロードされるAUXデータをダウンロードして記録することも可能とされている。

## 【0039】

IRD112は、電話回線104を介して課金サーバ105と通信可能とされている。IRD112には、各種情報が記憶されるICカードが挿入されるようになっている。そして、例えば楽曲のオーディオデータのダウンロードが行われたとすると、これに関する履歴情報がICカードに記憶される。このICカードの情報は、電話回線104を介して所定の機会、タイミングで課金サーバ105に送られる。課金サーバ105は、この送られてきた履歴情報に従って金額を設定して課金を行い、ユーザに請求する。

## 【0040】

これまでの説明から分かるように、本発明を適用したAVシステムを含むデジタル衛星放送システムでは、地上局101は、テレビ番組素材サーバ106からの音楽番組放送の素材となるビデオデータ及びオーディオデータと、楽曲素材サーバ107からのオーディオチャンネルの素材となるオーディオデータと、音声付加情報サーバ108からの音声データと、GUIデータサーバ109からのGUIデータとを多重化して送信している。

## 【0041】

そして、各家庭のAVシステム103でこの放送を受信すると、例えばモニタ装置114により、選局したチャンネルの番組を視聴することができる。また、番組のデータと共に送信されるGUIデータを利用したGUI画面として、EPG (Electrical Program Guide; 電子番組ガイド) 画面を表示させ、番組の検索等を行うことができる。また、例えば通常の番組放送以外の特定のサービス用のGUI画面を利用して所要の操作を行うことで、放送システムにおいて提供されている通常番組の視聴以外のサービスを享受することができる。

## 【0042】

例えば、オーディオ(楽曲)データのダウンロードサービス用のGUI画面を表示させて、このGUI画面を利用して操作を行えば、ユーザが希望した楽曲のオーディオデータをダウンロードしてMDレコーダ/プレーヤ1によりディスクに記録して保存することが可能になる。

【0 0 4 3】

ここで、このデジタル衛星放送システムでは、地上局 1 0 1 から衛星 1 0 2 を介しての A V システム 1 0 3 への送信を行うにあたり、D S M－C C（デジタル蓄積メディア・コマンド・アンド・コントロール；Digital Strage Media-Command and Control）プロトコルを採用する。

【0 0 4 4】

D S M－C C（M P E G－p a r t 6）方式は、既に知られているように、例えば、何らかのネットワークを介して、デジタル蓄積メディア（D S M）に蓄積された M P E G 符号化ビットストリームを取り出し（Retrieve）たり、或いは D S M に対してストリームを蓄積（Store）するためのコマンドや制御方式を規定したものである。

【0 0 4 5】

そして、D S M－C C 方式によりデータ放送サービス（例えば G U I 画面など）のコンテンツ（オブジェクトの集合）を伝送するためには、コンテンツの記述形式を定義しておく必要がある。このデジタル衛星放送システムでは、コンテンツの記述形式の定義として先に述べた M H E G が採用されている。

【0 0 4 6】

このデジタル衛星放送システムにおける地上局 1 0 1 は、図 2 のように構成されている。

【0 0 4 7】

図 2 に示した地上局 1 0 1 において、テレビ番組素材登録システム 1 3 1 は、テレビ番組素材サーバ 1 0 6 から得られた素材データを A V サーバ 1 3 5 に登録する。この素材データはテレビ番組送出システム 1 3 9 に送られ、ここでビデオデータは例えば M P E G 2 方式で圧縮され、オーディオデータは、例えば M P E G 2 オーディオ方式によりパケット化される。テレビ番組送出システム 1 3 9 の出力はマルチプレクサ 1 4 5 に送られる。

【0 0 4 8】

また、楽曲素材登録システム 1 3 2 では、楽曲素材サーバ 1 0 7 からの素材データ、つまりオーディオデータを、M P E G 2 オーディオエンコーダ 1 3 6 A、



及び ATRAC エンコーダ 136B に供給する。MPEG2 オーディオエンコーダ 136A、ATRAC エンコーダ 136B では、それぞれ供給されたオーディオデータについてエンコード処理（圧縮符号化）を行った後、MPEG オーディオサーバ 140A 及び ATRAC オーディオサーバ 140B に登録させる。

【0049】

MPEG オーディオサーバ 140A に登録された MPEG オーディオデータは、MPEG オーディオ送出システム 143A に伝送されてここでパケット化された後、マルチプレクサ 145 に伝送される。ATRAC オーディオサーバ 140B に登録された ATRAC データは、ATRAC オーディオ送出システム 143B に 4 倍速 ATRAC データとして送られ、ここでパケット化されてマルチプレクサ 145 に送出される。

【0050】

また、音声付加情報登録システム 133 では、音声付加情報サーバ 108 からの素材データである音声付加情報を音声付加情報データベース 137 に登録する。この音声付加情報データベース 137 に登録された音声付加情報は、音声付加情報送出システム 141 に伝送され、同様に、ここでパケット化されてマルチプレクサ 145 に伝送される。

【0051】

また、GUI 用素材登録システム 134 では、GUI データサーバ 109 からの素材データである GUI データを、GUI 素材データベース 138 に登録する。

【0052】

GUI 素材データベース 138 に登録された GUI 素材データは、GUI オーサリングシステム 142 に伝送され、ここで、GUI 画面としての出力が可能なデータ形式となるように処理が施される。

【0053】

つまり、GUI オーサリングシステム 142 に伝送されてくるデータとしては、例えば、楽曲のダウンロードのための GUI 画面であれば、アルバムジャケットの静止画像データ、歌詞などのテキストデータ、更には、操作に応じて出力さ

れるべき音声データなどである。

【 0 0 5 4 】

上記した各データはいわゆるモノメディアといわれるが、G U I オーサリングシステム 1 4 2 では、M H E G オーサリングツールを用いて、これらのモノメディアデータを符号化して、これをオブジェクトとして扱うようにする。

【 0 0 5 5 】

そして、G U I 画面の表示態様と操作に応じた画像音声の出力態様が得られるように上記オブジェクトの関係を規定したシナリオ記述ファイル（スクリプト）と共に M H E G - 5 のコンテンツを作成する。

【 0 0 5 6 】

また、テレビ番組素材サーバ 1 0 6 の素材データを基とする画像・音声データ（M P E G ビデオデータ、M P E G オーディオデータ）と、楽曲素材サーバ 1 0 7 の楽曲素材データを基とする M P E G オーディオデータ等も、G U I 画面に表示され、操作に応じた出力態様を与えられる。

【 0 0 5 7 】

従って、上記シナリオ記述ファイルとしては、上記 G U I オーサリングシステム 0 4 2 では、上記したテレビ番組素材サーバ 1 0 6 の素材データを基とする画像・音声データ、楽曲素材サーバ 1 0 7 の楽曲素材データを基とする M P E G オーディオデータ、更には、音声付加情報サーバ 1 0 8 を基とする音声付加情報も必要に応じてオブジェクトとして扱われて、M H E G のスクリプトによる規定が行われる。

【 0 0 5 8 】

なお、G U I オーサリングシステム 1 4 2 から伝送される M H E G コンテンツのデータとしては、スクリプトファイル、及びオブジェクトとしての各種静止画データファイルやテキストデータファイルなどとなるが、静止画データは、例えば J P E G (Joint Photograph Experts Group) 方式で圧縮された 6 4 0 × 4 8 0 ピクセルのデータとされ、テキストデータは例えば 8 0 0 文字以内のファイルとされる。

## 【0059】

GUIオーサリングシステム142にて得られたMHEGコンテンツのデータはDSM-CCエンコーダ144に伝送される。

## 【0060】

DSM-CCエンコーダ144では、MPEG2フォーマットに従ったビデオ、オーディオデータのデータストリームに多重できる形式のトランスポートストリーム（以下TS(Transport Stream)とも略す）に変換して、パケット化されてマルチプレクサ145に出力される。

## 【0061】

マルチプレクサ145においては、テレビ番組送出システム139からのビデオパケットおよびオーディオパケットと、MPEGオーディオ送出システム143Aからのオーディオパケットと、ATRACオーディオ送出システム143Bからの4倍速オーディオパケットと、音声付加情報送出システム141からの音声付加情報パケットと、GUIオーサリングシステム142からのGUIデータパケットとが時間軸多重化されると共に、キー情報サーバ110から出力されたキー情報に基づいて暗号化される。

## 【0062】

マルチプレクサ145の出力は電波送出システム146に伝送され、ここで例えば誤り訂正符号の付加、変調、及び周波数変換などの処理を施された後、アンテナから衛星102に向けて送信される。

## 【0063】

図3は、地上局101から衛星102に送信出力される際のデータの一例を示している。なお、この図3に示す各データは実際には時間軸多重化されているものである。また、各データは、図3に示すように、時刻 $t_1$ から時刻 $t_2$ の間が1つのイベントとされ、時刻 $t_2$ から次のイベントとされる。ここでいうイベントとは、例えば音楽番組のチャンネルであれば、複数楽曲のラインナップの組を変更する単位であり、時間的には30分或いは1時間程度となる。

## 【0064】

図3に示すように、時刻 $t_1$ から時刻 $t_2$ のイベントでは、通常の動画の番組

放送で、所定の内容 A 1 を有する番組が放送されている。また、時刻  $t_2$  から始めるイベントでは、内容 A 2 としての番組が放送されている。この通常の番組で放送されているのは動画と音声である。

## 【0065】

MPEGオーディオチャンネル(1)～(10)は、例えば、チャンネルCH1からCH10の10チャンネル分用意される。このとき、各オーディオチャンネルCH1, CH2, CH3・・・CH10では、1つのイベントが放送されている間は同一楽曲が繰り返し送信される。つまり、時刻  $t_1$  ～  $t_2$  のイベントの期間においては、オーディオチャンネルCH1では楽曲B1が繰り返し送信され、オーディオチャンネルCH2では楽曲C1が繰り返し送信され、以下同様に、オーディオチャンネルCH10では楽曲K1が繰り返し送信されることになる。これは、その下に示されている4倍速ATRACオーディオチャンネル(1)～(10)についても共通である。

## 【0066】

つまり、図3において、MPEGオーディオチャンネルと4倍速ATRACオーディオチャンネルのチャンネル番号である( )内の数字が同じものは同じ楽曲となる。また、音声付加情報のチャンネル番号である( )内の数字は、同じチャンネル番号を有するオーディオデータに付加されている音声付加情報である。更に、GUIデータとして伝送される静止画データやテキストデータも各チャンネルごとに形成されるものである。これらのデータは、図4の(a)～(d)に示すようにMPEG2のトランスポートパケット内で時分割多重されて送信され、図4の(e)～(h)に示すようにしてIRD112内では各データパケットのヘッダ情報を用いて再構築される。

## 【0067】

図5は、本発明に係るデータ伝送システムの構成を示すブロック図である。

## 【0068】

このデータ伝送システムは、上述のデジタル衛星放送システムに含まれたAVシステム103を構成するものであって、上記IRD112として機能するデータ送信装置10と上記MDレコーダ/プレーヤ1として機能するデータ受信装置

20を備え、上記データ送信装置10とデータ受信装置20が伝送路30を介して接続された構成となっている。

#### 【0069】

このデータ伝送システムにおいて、上記データ送信装置10は、通信衛星から送られてくる衛星デジタル多チャンネル放送番組を受信するセットトップボックスすなわち上述のIRD112であって、内部バス11に接続された中央演算処理ユニット(CPU: Central Processing Unit)12、メモリ13、入力インターフェース14、ユーザインターフェース15、入出力インターフェース16等により構成されている。上記入力インターフェース14には衛星アンテナ115が接続されている。また、上記入出力インターフェース16は、デジタルインターフェースであるIEEE(The International of Electrical and Electronics Engineers, Inc.)1394ハイ・パフォーマンス・シリアル・バス・インターフェース(以下、単にIEEE1394インターフェースという)であって、IEEE1394バスからなる上記伝送路30に接続されている。

#### 【0070】

このデータ送信装置10において、上記CPU12は、上記メモリ13に記憶されている制御プログラムにしたがって動作して、上記ユーザインターフェース15を介して入力される操作情報に応じて番組の選局動作等の各種制御動作を行うようになっている。

#### 【0071】

そして、このデータ送信装置10は、上記受信アンテナ115が接続された上記入力インターフェース14により衛星デジタル多チャンネル放送信号の所望のチャンネルを選局して所望のチャンネルのコンテンツ(音楽データ)及びメタデータ(テキストデータやJPEGデータ等の関連データ)を受信し、受信した音楽データ及びメタデータ(関連データ)を上記入出力インターフェース16から上記伝送路30に送信する。

#### 【0072】

また、上記データ受信装置20は、上記データ送信装置10すなわちセットトップボックスにより受信したコンテンツ(音楽データ)及びメタデータ(関連デ

ータ) を磁気テープや光磁気ディスクなどの記録媒体を介して記録／再生する記録／再生装置であって、内部バス 2 1 に接続された中央演算処理ユニット (CPU: Central Processing Unit) 2 2、メモリ 2 3、入出力インターフェース 2 4、ユーザインターフェース 2 5、メディアアクセス部 2 6 等により構成されている。上記入出力インターフェース 2 4 は、デジタルインターフェースである I E E E (The International of Electrical and Electronics Engineers, Inc.) 1 3 9 4 ハイ・パフォーマンス・シリアル・バス・インターフェース (以下、単に I E E E 1 3 9 4 インターフェースという) であって、I E E E 1 3 9 4 バスからなる上記伝送路 3 0 が接続されている。

【0073】

図 6 は、上記伝送路 3 0 として実際に用いられる I E E E 1 3 9 4 バスカーブルの構造例を示している。

【0074】

この図 6 においては、コネクタ 6 0 0 A と 6 0 0 B がケーブル 6 0 1 を介して接続されていると共に、ここでは、コネクタ 6 0 0 A と 6 0 0 B のピン端子として、ピン番号 1 ～ 6 の 6 ピンが使用される場合を示している。

【0075】

コネクタ 6 0 0 A、6 0 0 B に設けられる各ピン端子については、ピン番号 1 は電源 (V P)、ピン番号 2 はグランド (V G)、ピン番号 3 は T P B 1、ピン番号 4 は T P B 2、ピン番号 5 は T P A 1、ピン番号 5 は T P A 2 とされている。

【0076】

そして、コネクタ 6 0 0 A - 6 0 0 B 間の各ピンの接続形態は、

ピン番号 1 (V P) - ピン番号 1 (V P)

ピン番号 2 (V G) - ピン番号 2 (V G)

ピン番号 3 (T P B 1) - ピン番号 5 (T P A 1)

ピン番号 4 (T P B 2) - ピン番号 6 (T P A 2)

ピン番号 5 (T P A 1) - ピン番号 3 (T P B 1)

ピン番号 6 (T P A 2) - ピン番号 3 (T P B 2)

のようになっている。そして、上記ピン接続の組のうち、

ピン番号3 (TPB1) - ピン番号5 (TPA1)

ピン番号4 (TPB2) - ピン番号6 (TPA2)

の2本のツイスト線の組により、差動で信号を相互伝送する信号線601Aを形成し、

ピン番号5 (TPA1) - ピン番号3 (TPB1)

ピン番号6 (TPA2) - ピン番号3 (TPB2)

の2本のツイスト線の組により、差動で信号を相互伝送する信号線601Bを形成している。

#### 【0077】

上記2組の信号線601A及び信号線601Bにより伝送される信号は、図7の(a)に示すデータ信号(Data)と、図7の(b)に示すストロブ信号(Strobe)である。

#### 【0078】

図7の(a)に示すデータ信号は、信号線601A又は信号線601Bの一方を使用してTPB1, 2から出力され、TPA1, 2に入力される。

#### 【0079】

また、図7の(b)に示すストロブ信号は、データ信号と、このデータ信号に同期する伝送クロックとについて所定の論理演算を行うことによって得られる信号であり、実際の伝送クロックよりは低い周波数を有する。このストロブ信号は、信号線601A又は信号線601Bのうち、データ信号伝送に使用していない他方の信号線を使用して、TPA1, 2から出力され、TPB1, 2に入力される。

#### 【0080】

例えば、図7の(a), (b)に示すデータ信号及びストロブ信号が、或るIEEE1394対応の機器に対して入力されたとすると、この機器においては、入力されたデータ信号とストロブ信号とについて所定の論理演算を行って、図7の(c)に示すような伝送クロック(Clock)を生成し、所要の入力データ信号処理に利用する。

【 0 0 8 1 】

IEEE 1 3 9 4 規格では、このようなハードウェア的データ伝送形態を採ることで、高速な周期の伝送クロックをケーブルによって機器間で伝送する必要をなくし、信号伝送の信頼性を高めるようにしている。

【 0 0 8 2 】

なお、上記説明では6ピンの仕様について説明したが、IEEE 1 3 9 4 フォーマットでは電源 (VP) とグランド (VG) を省略して、2組のツイスト線である信号線 6 0 1 A 及び信号線 6 0 1 B のみからなる4ピンの仕様も存在する。例えば、このAVシステム 1 0 3 におけるMDレコーダ/プレーヤ 1 では、実際には、この4ピン仕様のケーブルを用いることで、ユーザにとってより簡易なシステムを提供できるように配慮している。

【 0 0 8 3 】

ここで、IEEE 1 3 9 4 規格では、IEEE 1 3 9 4 バスを介して接続されたネットワーク内で行われる伝送動作をサブアクションと呼び、次の2種類のサブアクションが規定されている。すなわち、2つのサブアクションとして、「アシンクロナス (Asynchronous)」と呼ばれる非同期伝送モード、及び、「アイソクロナス (Isochronous)」と呼ばれる伝送帯域を保証した同期伝送モードが定義されている。

【 0 0 8 4 】

すなわち、IEEE 1 3 9 4 規格では、図 8 に示すように Isochronous cycle (nominal cycle) の周期を繰り返すことによって送信を行う。この場合、1 Isochronous cycle は、 $125 \mu \text{sec}$  とされ、帯域としては  $100 \text{MHz}$  に相当する。なお、Isochronous cycle の周期としては  $125 \mu \text{sec}$  以外とされても良いことが規定されている。そして、この Isochronous cycle ごとに、データをパケット化して送信する。

【 0 0 8 5 】

この Isochronous cycle の先頭には、1 Isochronous cycle の開始を示す Cycle Start Packet が配置される。



## 【0086】

このCycle Start Packetは、Cycle Masterとして定義されたIEEE 1394 ネットワークシステム内の特定の1機器によってその発生タイミングが指示される。

## 【0087】

Cycle Start Packetに続いては、Isochronous Packetが優先的に配置される。Isochronous Packetは、図8のように、チャンネルごとにパケット化されたうえで時分割的に配列されて転送される(Isochronous subactions)。また、Isochronous subactions内においてパケット毎の区切りには、Isochronous gap といわれる休止区間（例えば0.05  $\mu$ sec）が設けられる。

## 【0088】

このように、IEEE 1394 システムでは、1つの伝送線路によってIsochronous データをマルチチャンネルで送受信することが可能とされている。

## 【0089】

ここで、例えばこのAVシステムにおけるMDレコーダ/プレーヤ1が対応するATRACデータ（圧縮オーディオデータ）をIsochronous 方式により送信することを考えた場合、ATRACデータが1倍速の転送レート1.4 Mbpsであるとすれば、125  $\mu$ secである1 Isochronous cycle 周期ごとに、少なくともほぼ20数MバイトのATRACデータをIsochronous Packetとして伝送すれば、時系列的な連続性（リアルタイム性）が確保されることになる。

## 【0090】

例えば、或る機器がATRACデータを送信する際には、IEEE 1394 ネットワークシステム内のIRM(Isochronous Resource Manager)に対して、ATRACデータのリアルタイム送信が確保できるだけの、Isochronous パケットのサイズを要求する。IRMでは、現在のデータ伝送状況を監視して許可/不許可を与え、許可が与えられれば、指定されたチャンネルによって、ATRACデータをIsochronous Packetにパケット化して送信することが出来る。これがIEEE 1394 インターフェイスにおける帯域予約といわれるものである。

【0091】

Isochronous cycle の帯域内においてIsochronous subactionsが使用していない残りの帯域を用いて、Asynchronous subactions、即ちAsynchronous のパケット送信が行われる。

【0092】

図8では、Packet A, Packet B の2つのAsynchronous Packetが送信されている例が示されている。Asynchronous Packet の後には、ack gap(0.05  $\mu$ sec)の休止期間を挟んで、ACK (Acknowledge) といわれる信号が付随する。ACKは、Asynchronous Transactionの過程において、何らかのAsynchronousデータの受信があったことを送信側(Controller)に知らせるためにハードウェア的に受信側(Target)から出力される信号である。

【0093】

また、Asynchronous Packet 及びこれに続くACKからなるデータ伝送単位の前後には、10  $\mu$ sec程度のsubaction gap といわれる休止期間が設けられる。

【0094】

ここで、Isochronous PacketによりATRA Cデータを送信し、上記ATRA Cデータに付随するAUXデータファイルをAsynchronous Packet により送信するようにすれば、見かけ上、ATRA CデータとAUXデータファイルとを同時に送信することが可能となる。

【0095】

ここで、Asynchronous伝送は1対1のユニキャスト伝送であり、ブロードキャスト伝送を行うIsochronous 伝送に比べて盗聴が難しいという性質がある。

【0096】

このデータ伝送システムでは、伝送帯域を確保できるIsochronous 伝送を用いて音楽データを伝送し、関連情報は、Asynchronous 伝送を用いて伝送する。

【0097】

そして、データ受信装置20は、入出力インターフェース24を介して音楽データと関連情報を受信し、それが記録可能であれば、メディアアクセス部26に

より上記磁気テープや光磁気ディスクなどの記録媒体に記録する。

【0098】

上記記録媒体に記録された音楽データと関連情報はメディアアクセス部26により再生され、音楽データは、アナログ信号に変換されアナログ音声出力端子26Aから出力され、関連データは映像出力端子26Bから出力される。また、上記メディアアクセス部26により再生され音楽データと関連情報は、IEEE1394インターフェースを介してさらに他の機器に伝送されることがある。

【0099】

また、データ受信装置20は、記録禁止の音楽データを受信した場合には、上記メディアアクセス部26により記録媒体に記録することなく、単に音楽データをアナログ信号に変換してアナログ音声出力端子26Aから出力する。

【0100】

このデータ受信装置20において、上記CPU22は、上記メモリ23に記憶されている制御プログラムにしたがって動作して、上記ユーザインターフェース25を介して入力される操作情報に応じて、上記メディアアクセス部26による記録動作等の各種制御動作を行うようになっている。

【0101】

そして、このデータ伝送システムでは、受信アンテナ115を介してデータ送信装置10により受信した所望のチャンネルのコンテンツ（音楽データ）及びメタデータ（関連データすなわちテキストデータやJPEGデータ等）を、それぞれ別の暗号方式、暗号鍵を用いて暗号化してデータ受信装置20に伝送する。

【0102】

すなわち、データ送信装置10の要部構成を図9に示してあるように、上記データ送信装置10の入力インターフェース14は、衛星デジタル多チャネル放送信号の所望のチャンネルを選局するデマルチプレクサ(DEMUX)14Aと、このデマルチプレクサ(DEMUX)14Aにより選局された所望のチャンネルのトランスポートストリームを復号するデコーダ(DEC)14Bを備え、また、入出力インターフェース16は、上記デコーダ(DEC)14Bにより復号された所望のチャンネルのトランスポートストリームに含まれているコンテンツ（音楽データ）及びメタ

データ（関連データすなわちテキストデータやJ P E Gデータ等）を分離するデータ分離回路16Aと、このデータ分離回路16Aにより分離されたコンテンツ（音楽データ）を暗号鍵Kisoにより第1の暗号方式で暗号化してIsochronous Packetを生成する第1のエンコーダ16Bと、上記データ分離回路16Aにより分離されたメタデータ（関連データ）を暗号鍵Kasyncにより第2の暗号方式で暗号化してAsynchronous Packetを生成する第1のエンコーダ16Cを備える。

## 【0103】

そして、上記データ送信装置10における入出力インターフェース16は、CPU12により制御されて、図10のフローチャートに示すように動作する。すなわち、上記入出力インターフェース16は、上記入力インターフェース14を介して受信された所望のチャンネルのトランスポートストリームが入力されると（ステップS1）、入力されたトランスポートストリームに含まれているデータがコンテンツ（音楽データ）であるかメタデータ（関連データ）であるかを判定し（ステップS2）、コンテンツ（音楽データ）である場合には、そのコンテンツ（音楽データ）を暗号鍵Kisoにより第1の暗号方式で暗号化し（ステップS3）、第1の暗号方式で暗号化したコンテンツ（音楽データ）をIsochronous Packetとして伝送する処理を行う（ステップS4）。また、入力されたトランスポートストリームに含まれているデータがメタデータ（関連データ）である場合には、そのメタデータ（関連データ）を暗号鍵KAsyncにより第2の暗号方式で暗号化し（ステップS5）、第2の暗号方式で暗号化したメタデータ（関連データ）をAsynchronous Packetとして伝送する処理を行う（ステップS6）。

## 【0104】

このデータ伝送システムでは、上記データ伝送に先立って、データ送信装置10とデータ受信装置20の間で相互認証と2種類の暗号鍵の共有プロトコルを実行する。具体的には、図11のフローチャートに示すような認証・鍵共有プロトコルを実行してから、データ伝送を行う。なお、このデータ伝送システムにおけるデータ送信装置10側の処理手順を図12のフローチャートに示すとともに、データ受信装置20側の処理手順を図13のフローチャートに示す。

## 【0105】

上記認証・鍵共有プロトコルを示す図11では、データ送信装置10をSource DeviceAで表し、データ受信装置20をSink DeviceBで表す。これらの機器は、自分が正当であることを示す情報Kvが機器の製造時に与えられ、秘密に保持している。

## 【0106】

そして、このデータ伝送システムにおいて、上記データ送信装置10すなわちセットトップボックスのCPU12は、先ず、データの伝送を開始するためのスタートコマンドを上記入出力インターフェース16から上記伝送路30を介してデータ受信装置20に送信する（ステップS10）。

## 【0107】

上記データ受信装置20すなわち記録装置のCPU22は、上記入出力インターフェース24に接続された上記伝送路30を介して上記データ送信装置10から送られてくるスタートコマンド(START command)を受信したら（ステップS20）、認証・鍵共有プロトコルの開始要求(Request authentication)とm（例えばm=64）ビットの2つの乱数Bn1, Bn2を生成して上記データ送信装置10に入出力インターフェース24を介して送る（ステップS21）。

## 【0108】

上記データ送信装置10のCPU12は、上記入出力インターフェース14に接続された上記伝送路30を介して上記データ受信装置20から送られてくる認証・鍵共有プロトコルの開始要求(Request authentication)と乱数Bn1, Bn2を受信したら（ステップS11）、mビットの2つの乱数An1, An2を生成して上記データ受信装置10に入出力インターフェース14を介して送る（ステップS12）。

## 【0109】

上記データ受信装置10は、上記データ送信装置10から送られてくる2つの乱数An1, An2を受信する（ステップS22）。

## 【0110】

そして、上記データ送信装置10のCPU12は、自分が正当であることを示

す情報  $K_v$  と上記ステップ S 1 2 でデータ受信装置 2 0 に送った乱数  $A_{n2}$  と上記ステップ S 1 1 で受信した乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) をハッシュ関数  $H a s h []$  に入力し、

$$R2 = H a s h [K_v \parallel A_{n2} \parallel B_{n2}]_{msb\_m}$$

その出力の最上位  $m$  ビットをレスポンスデータ  $R2$  とし、このレスポンスデータ  $R2$  を上記データ受信装置 2 0 に入出力インターフェース 1 4 を介して送る (ステップ S 1 3)。ここで、 $X \parallel Y$  は、 $X$  と  $Y$  とのビット連結を示す。

【0 1 1 1】

上記データ受信装置 2 0 の CPU 2 2 は、上記データ送信装置 1 0 から送られてくるレスポンスデータ  $R2$  を受信し (ステップ S 2 3)、自分が正当であることを示す情報  $K_v$  と上記ステップ S 2 2 で受信した乱数  $A_{n1}$  と上記ステップ S 2 1 でデータ送信装置 1 0 に送った乱数  $A_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) をハッシュ関数  $H a s h []$  に入力し、

$$R1 = H a s h [K_v \parallel A_{n1} \parallel B_{n1}]_{msb\_m}$$

その出力の最上位  $m$  ビットをレスポンスデータ  $R1$  とし、このレスポンスデータ  $R1$  を上記データ送信装置 1 0 に入出力インターフェース 2 4 を介して送る (ステップ S 2 4)。

【0 1 1 2】

上記データ送信装置 1 0 の CPU 1 2 は、上記データ受信装置 2 0 から送られてくるレスポンスデータ  $R1$  を受信する (ステップ S 1 4)。

【0 1 1 3】

さらに、上記データ送信装置 1 0 の CPU 1 2 は、自分が正当であることを示す情報  $K_v$  と上記ステップ S 1 2 でデータ受信装置 2 0 に送った乱数  $A_{n1}$  と上記ステップ S 1 1 で受信した乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) をハッシュ関数  $H a s h []$  に入力し、

$$R'1 = H a s h [K_v \parallel A_{n1} \parallel B_{n1}]_{msb\_m}$$

その出力の最上位 $m$ ビットを参照データ $R'1$ とする(ステップS15)。

【0114】

そして、上記データ送信装置10のCPU12は、上記参照データ $R'1$ を上記ステップS14で受信したレスポンスデータ $R1$ と比較する(ステップS16)。このステップS16において、レスポンスデータ $R1$ が参照データ $R'1$ と一致しなければ、上記データ送信装置10のCPU12は、上記データ受信装置20が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

【0115】

上記ステップS16においてレスポンスデータ $R1$ が参照データ $R'1$ と一致した場合には、上記データ送信装置10のCPU12は、上記データ受信装置20を正当な機器であると判断し、自分が正当であることを示す情報 $Kv$ と上記ステップS12でデータ受信装置20に送った乱数 $An1$ と上記ステップS11で受信した乱数 $Bn1$ を連結した連結データ( $Kv \parallel An1 \parallel Bn1$ )をハッシュ関数 $Hash[]$ に入力し、

$$Kiso = Hash[Kv \parallel An1 \parallel Bn1]_{lsb\_m}$$

その出力の最下位 $m$ ビットをIsochronous 伝送で送るデータを暗号化するために使用する暗号鍵 $Kiso$ とする。また、上記データ送信装置10のCPU12は、自分が正当であることを示す情報 $Kv$ と上記ステップS12でデータ受信装置20に送った乱数 $An2$ と上記ステップS11で受信した乱数 $Bn2$ を連結した連結データ( $Kv \parallel An2 \parallel Bn2$ )をハッシュ関数 $Hash[]$ に入力し、

$$Kasync = Hash[Kv \parallel An2 \parallel Bn2]_{lsb\_m}$$

その出力の最下位 $m$ ビットをAsynchronous伝送で送るデータを暗号化するために使用する暗号鍵 $Kasync$ とする(ステップS17)。

【0116】

また、上記データ受信装置20のCPU22は、自分が正当であることを示す情報 $Kv$ と上記ステップS22で受信した乱数 $An2$ と上記ステップS21でデータ送信装置10に送った乱数 $Bn2$ を連結した連結データ( $Kv \parallel An2 \parallel Bn2$ )を生成し、この連結データ( $Kv \parallel An2 \parallel Bn2$ )をハッシュ関数 $Hash[]$ に入力し、

$$R'2 = \text{Hash}[Kv \parallel An2 \parallel Bn2]_{\text{msb}_m}$$

その出力の最上位 $m$ ビットを参照データ $R'2$ とする（ステップS25）。

【0117】

そして、上記データ受信装置20のCPU22は、この参照データ $R'2$ を上記ステップS23で受信したレスポンスデータ $R2$ と比較する（ステップS26）。このステップS26において、レスポンスデータ $R2$ が参照データ $R'2$ と一致しなければ、上記データ受信装置20のCPU22は、上記データ送信装置10が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

【0118】

また、上記ステップS26においてレスポンスデータ $R2$ が参照データ $R'2$ と一致した場合には、上記データ受信装置20のCPU22は、上記データ送信装置10を正当な機器であると判断し、自分が正当であることを示す情報 $Kv$ と上記ステップS22で受信した乱数 $An1$ と上記ステップS21でデータ送信装置10に送った乱数 $Bn1$ を連結した連結データ( $Kv \parallel An1 \parallel Bn1$ )をハッシュ関数 $\text{Hash}[]$ に入力し、

$$K'_{\text{iso}} = \text{Hash}[Kv \parallel An1 \parallel Bn1]_{\text{lsb}_m}$$

その出力の最下位 $m$ ビットを $\text{Isochronous}$ 伝送で送られてくるデータを復号するために使用する暗号鍵 $K'_{\text{iso}}$ とする。また、自分が正当であることを示す情報 $Kv$ と上記ステップS22で受信した乱数 $An2$ と上記ステップS21でデータ送信装置10に送った乱数 $Bn2$ を連結した連結データ( $Kv \parallel An2 \parallel Bn2$ )をハッシュ関数 $\text{Hash}[]$ に入力し、

$$K'_{\text{async}} = \text{Hash}[Kv \parallel An2 \parallel Bn2]_{\text{lsb}_m}$$

その出力の最下位 $m$ ビットを $\text{Asynchronous}$ 伝送で送られてくるデータを復号するために使用する暗号鍵 $K'_{\text{async}}$ とする（ステップS27）。

【0119】

このデータ伝送システムでは、データ伝送に先立って、上記認証・鍵共有プロトコルをデータ送信装置10とデータ受信装置20の間でIEEE1394の $\text{Asynchronous}$ 伝送によって実行することにより、データ送信装置10とデータ受信装置20が、相互に正当性を認証するとともに、 $\text{Isochronous}$ 伝送で暗号化した



データを送るための暗号鍵と Asynchronous 伝送で暗号化したデータを送るための暗号鍵を共有することができる。

#### 【0 1 2 0】

そして、このデータ伝送システムでは、上記認証・鍵共有プロトコルを実行した後、データ送信装置 1 0 から音楽データを暗号鍵 K iso で暗号化して Isochronous 伝送で送信し、また、関連データを暗号鍵 K async で暗号化して Asynchronous 伝送で送信し（ステップ S 1 8）、データ受信装置 2 0 は、Isochronous 伝送により送られてくる音楽データを暗号鍵 K' iso で復号し、また、Asynchronous 伝送で送られてくる関連データを暗号鍵 K' async で復号する（ステップ S 2 8）。

#### 【0 1 2 1】

すなわち、上記認証・鍵共有プロトコルの実行後は、データ受信装置 2 0 は、データ送信装置 1 0 から Isochronous 伝送により送られてくる音楽データを暗号鍵 K' iso で復号し、また、Asynchronous 伝送で送られてくる関連データを暗号鍵 K' async で復号して、それぞれの平文データを得ることができる。

#### 【0 1 2 2】

ここで、このデータ伝送システムにおいて、上記データ伝送に先立って実行する認証・鍵共有プロトコルの他の例を図 1 4 のフローチャートに示す。この場合のデータ送信装置 1 0 側の処理手順を図 1 5 のフローチャートに示すとともに、データ受信装置 2 0 側の処理手順を図 1 6 のフローチャートに示す。

#### 【0 1 2 3】

上記認証・鍵共有プロトコルを示す図 1 4 では、データ送信装置 1 0 を Source Device A で表し、データ受信装置 2 0 を Sink Device B で表す。これらの機器は、自分が正当であることを示す情報 K v が機器の製造時に与えられ、秘密に保持している。

#### 【0 1 2 4】

そして、このデータ伝送システムにおいて、上記データ送信装置 1 0 すなわちセットトップボックスの CPU 1 2 は、先ず、データの伝送を開始するためのスタートコマンドを上記入出インターフェース 1 6 から上記伝送路 3 0 を介してデ

ータ受信装置 2 0 に送信する (ステップ S 1 1 0)。

【 0 1 2 5 】

上記データ受信装置 2 0 すなわち記録装置の CPU 2 2 は、上記入出力インターフェース 2 4 に接続された上記伝送路 3 0 を介して上記データ送信装置 1 0 から送られてくるスタートコマンド (START command) を受信したら (ステップ S 1 2 0)、認証・鍵共有プロトコルの開始要求 (Request authentication) と  $m$  (例えば  $m = 64$ ) ビットの 2 つの乱数  $B_{n1}$ ,  $B_{n2}$  を生成して上記データ送信装置 1 0 に入出力インターフェース 2 4 を介して送る (ステップ S 1 2 1)。

【 0 1 2 6 】

上記データ送信装置 1 0 の CPU 1 2 は、上記入出力インターフェース 1 4 に接続された上記伝送路 3 0 を介して上記データ受信装置 2 0 から送られてくる認証・鍵共有プロトコルの開始要求 (Request authentication) と乱数  $B_{n1}$ ,  $B_{n2}$  を受信したら (ステップ S 1 1 1)、 $m$  ビットの 2 つの乱数  $A_{n1}$ ,  $A_{n2}$  を生成して上記データ受信装置 1 0 に入出力インターフェース 1 4 を介して送る (ステップ S 1 1 2)。

【 0 1 2 7 】

上記データ受信装置 1 0 は、上記データ送信装置 1 0 から送られてくる 2 つの乱数  $A_{n1}$ ,  $A_{n2}$  を受信する (ステップ S 1 2 2)。

【 0 1 2 8 】

そして、上記データ送信装置 1 0 の CPU 1 2 は、自分が正当であることを示す情報  $K_v$  と上記ステップ S 1 1 2 でデータ受信装置 2 0 に送った乱数  $A_{n1}$  と上記ステップ S 1 1 1 で受信した乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) をハッシュ関数 Hash [ ] に入力し、

$$R'_{1} = \text{Hash} [K_v \parallel A_{n1} \parallel B_{n1}]_{\text{msb}_p}$$

その出力の最上位  $p$  ビット (例えば  $p = 64$ ) を参照データ  $R'_{1}$  とするとともに、

$$K_{iso} = \text{Hash} [K_v \parallel A_{n1} \parallel B_{n1}]_{\text{lsb}_n}$$

最下位  $n$  (例えば  $n = 64$ ) ビットを Isochronous 伝送で送るデータを暗号化す

るために使用する暗号鍵  $K_{iso}$  とする（ステップ S113）。ここで、 $X \parallel Y$  は、 $X$  と  $Y$  とのビット連結を示す。

【0129】

そして、上記データ送信装置 10 の CPU12 は、このようにして算出した暗号鍵  $K_{iso}$  と上記ステップ S112 でデータ受信装置 20 に送った乱数  $A_{n1}$  と上記ステップ S111 で受信した乱数  $B_{n1}$  を連結した連結データ ( $K_{iso} \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_{iso} \parallel A_{n1} \parallel B_{n1}$ ) をハッシュ関数  $Hash[]$  に入力し、

$$R2 = Hash[K_{iso} \parallel A_{n1} \parallel B_{n1}]_{msb\_p}$$

その出力の最上位  $p$  ビットをレスポンスデータ  $R2$  とする（ステップ S114）

また、上記データ受信装置 20 の CPU22 は、自分が正当であることを示す情報  $K_v$  と上記ステップ S122 で受信した乱数  $A_{n1}$  と上記ステップ S121 でデータ送信装置 10 に送った乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) をハッシュ関数  $Hash[]$  に入力し、

$$R1 = Hash[K_v \parallel A_{n1} \parallel B_{n1}]_{msb\_p}$$

その出力の最上位  $p$  ビットをレスポンスデータ  $R1$  とし、

$$K'_{iso} = Hash[K_v \parallel A_{n1} \parallel B_{n1}]_{lsb\_n}$$

最下位  $n$  ビットを *Isochronous* 伝送で送られてくるデータを復号するために使用する暗号鍵  $K'_{iso}$  とする（ステップ S123）。

【0130】

また、上記データ受信装置 20 の CPU22 は、このようにして算出した暗号鍵  $K'_{iso}$  と上記ステップ S122 で受信した乱数  $A_{n2}$  と上記ステップ S121 でデータ送信装置 10 に送った乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) をハッシュ関数  $Hash[]$  に入力し、

$$R'2 = Hash[K'_{iso} \parallel A_{n2} \parallel B_{n2}]_{msb\_p}$$

その出力の最上位  $p$  ビットを参照データ  $R'2$  とする（ステップ S124）。

【0131】

そして、上記データ送信装置10のCPU12は、ステップS114で算出したレスポンスデータR2を上記データ受信装置20に入出力インターフェース14を介して送る（ステップS115）。

【0132】

上記データ受信装置20のCPU22は、上記データ送信装置10から送られてくるレスポンスデータR2を受信し（ステップS125）、上記ステップS124で算出した参照R'2と比較する（ステップS126）。このステップS126において、レスポンスデータR1が参照データR'1と一致しなければ、上記データ受信装置20のCPU22は、上記データ送信装置10が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

【0133】

上記ステップS126においてレスポンスデータR2が参照データR'2と一致した場合には、上記データ受信装置20のCPU22は、上記ステップS123で算出したレスポンスデータR1を上記データ送信装置10に入出力インターフェース14を介して送る（ステップS127）。

【0134】

上記データ送信装置10のCPU10は、上記データ受信装置20から送られてくるレスポンスデータR1を受信し（ステップS116）、上記ステップS113で算出した参照データR'1と比較する（ステップS117）。このステップS117において、レスポンスデータR1が参照データR'1と一致しなければ、上記データ送信装置20のCPU12は、上記データ受信装置20が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

【0135】

上記ステップS117においてレスポンスデータR1が参照データR'1と一致した場合には、上記データ送信装置10のCPU12は、上記データ受信装置20を正当な機器であると判断し、上記ステップS113で算出した暗号鍵Kisoと上記ステップS112でデータ受信装置20に送った乱数An2と上記ステップS111で受信した乱数Bn2を連結した連結データ（Kiso || An2 || B

$n 2$ )を生成し、この連結データ ( $K_{iso} \parallel A_{n 2} \parallel B_{n 2}$ )をハッシュ関数  $H a s h [ ]$  に入力し、

$$K_{async} = H a s h [ K_{iso} \parallel A_{n 2} \parallel B_{n 2} ] l s b _ q$$

その出力の最下位  $q$  ビット (例えば  $q = 64$ ) を Asynchronous 伝送で送るデータを暗号化するために使用する暗号鍵  $K_{async}$  とする (ステップ S 1 1 8)。

【 0 1 3 6 】

また、上記データ受信装置 2 0 の CPU 2 2 は、上記ステップ S 1 2 3 で算出した暗号鍵  $K'_{iso}$  と上記ステップ S 1 2 2 で受信した乱数  $A_{n 2}$  と上記ステップ S 1 2 1 でデータ送信装置 1 0 に送った乱数  $B_{n 2}$  を連結した連結データ ( $K'_{iso} \parallel A_{n 2} \parallel B_{n 2}$ ) を生成し、この連結データ ( $K'_{iso} \parallel A_{n 2} \parallel B_{n 2}$ ) をハッシュ関数  $H a s h [ ]$  に入力し、

$$K'_{async} = H a s h [ K'_{iso} \parallel A_{n 2} \parallel B_{n 2} ] l s b _ q$$

その出力の最下位  $q$  ビットを Asynchronous 伝送で送られてくるデータを復号するために使用する暗号鍵  $K'_{async}$  とする (ステップ S 1 2 8)。

【 0 1 3 7 】

このデータ伝送システムでは、データ伝送に先立って、上記認証・鍵共有プロトコルをデータ送信装置 1 0 とデータ受信装置 2 0 の間で IEEE 1 3 9 4 の Asynchronous 伝送によって実行することにより、データ送信装置 1 0 とデータ受信装置 2 0 が、相互に正当性を認証するとともに、Isochronous 伝送で暗号化したデータを送るための暗号鍵と Asynchronous 伝送で暗号化したデータを送るための暗号鍵を共有することができる。

【 0 1 3 8 】

すなわち、上記認証・鍵共有プロトコルの実行後は、データ送信装置 1 0 から音楽データを暗号鍵  $K_{iso}$  で暗号化して Isochronous 伝送で送信し、また、関連データを暗号鍵  $K_{async}$  で暗号化して Asynchronous 伝送で送信することによって (ステップ S 1 1 9)、データ受信装置 2 0 は、Isochronous 伝送により送られてくる音楽データを暗号鍵  $K'_{iso}$  で復号し、また、Asynchronous 伝送で送られてくる関連データを暗号鍵  $K'_{async}$  で復号することにより (ステップ S 1 2 9)、それぞれの平文データを得ることができる。

## 【0 1 3 9】

ここで、一般にIsochronous 伝送とAsynchronous伝送では性質が違っているので、それぞれに用いられる暗号アルゴリズムやモードもそれぞれに適したものが使用される。そこで、Asynchronous伝送に使用される暗号アルゴリズムがIsochronous 伝送に使用されるものに比べて強度的に弱い場合、Asynchronous伝送に使用される暗号鍵K<sub>async</sub>は、Isochronous 伝送に使用される暗号鍵K<sub>iso</sub>に比べて比較的容易に露呈してしまうことになる。図 1 1 に示した認証・鍵共有プロトコルでは、各機器が秘密に保持している自分が正当であることを示す情報K<sub>v</sub>から暗号鍵K<sub>async</sub>と暗号鍵K<sub>iso</sub>を直接生成しているので、暗号鍵K<sub>async</sub>が露呈してしまうと、例えば総当たり攻撃により情報K<sub>v</sub>が露呈してしまうことになる。

## 【0 1 4 0】

これに対して、図 1 4 に示した認証・鍵共有プロトコルでは、各機器が秘密に保持している自分が正当であることを示す情報K<sub>v</sub>から暗号鍵K<sub>iso</sub> を生成し、この暗号鍵K<sub>iso</sub> から暗号鍵K<sub>async</sub>を生成しているので、暗号鍵K<sub>async</sub>が露呈しても、攻撃者は、一方向性関数H a s hを一度攻撃するだけでは情報K<sub>v</sub>を得ることはできず、総当たり攻撃により暗号鍵K<sub>iso</sub> を求めて、しかる後に情報K<sub>v</sub>を総当たり攻撃しなければならない。

## 【0 1 4 1】

すなわち、図 1 4 に示した認証・鍵共有プロトコルでは、図 1 1 に示した認証・鍵共有プロトコルと比較して、各機器が秘密に保持している自分が正当であることを示す情報K<sub>v</sub>が露呈しにくく、伝送帯域の保証が必要なデータと上記データに関する関連データを安全にかつ確実に伝送することができる。

## 【0 1 4 2】

なお、上述のデータ伝送システムでは、各認証・鍵共有プロトコルを実行することによりデータ送信装置 1 0 とデータ受信装置 2 0 の間で共有される暗号鍵K<sub>iso</sub>, K'<sub>iso</sub> 及び暗号鍵K<sub>async</sub>, K'<sub>async</sub> を用いて伝送データを暗号化／復号するようにしているが、実際に伝送するデータを暗号化／復号するための暗号鍵（コンテンツキー）は別に用意して、暗号鍵K<sub>iso</sub>, K'<sub>iso</sub> 及び暗号鍵K<sub>async</sub>, K'<sub>async</sub>を用いてコンテンツキーをデータ送信装置 1 0 とデータ受信装置 2 0

の間で共有することもできる。

【0 1 4 3】

【発明の効果】

以上のように本発明では、伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースを介して、伝送帯域の保証が必要なデータを第 1 の伝送モードで伝送し、上記データに関する関連データを第 2 の伝送モードで伝送するので、伝送帯域が確保された伝送方式と伝送帯域が確保されていない伝送方式の 2 種類の伝送方式を採用して、データを確実に伝送することができる。

【0 1 4 4】

また、本発明では、上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で暗号化して第 1 の伝送モードで伝送し、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで伝送するにより、伝送帯域の保証が必要なデータと上記データに関する関連データを安全に伝送することができる。

【0 1 4 5】

さらに、本発明では、データ伝送に先立って、データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行することによって、データ送信装置とデータ受信装置が互いの正当性を認証するとともに、暗号鍵を共有することができ、伝送帯域の保証が必要なデータと上記データに関する関連データを安全にかつ確実に伝送することができる。

【図面の簡単な説明】

【図 1】

本発明を適用した A V システムを含むデジタル衛星放送システムの全体構成をブロック図である。

【図 2】

上記デジタル衛星放送システムにおける地上局の構成をブロック図である。

【図 3】

上記地上局から送信されるデータを示す図である。

【図 4】

送信データの時分割多重化構造を示す説明図である。

【図 5】

本発明を適用したデータ伝送システムの構成を示すブロック図である。

【図 6】

IEEE 1394 バスケーブルの構造を模式的に示す説明図である。

【図 7】

IEEE 1394 における信号伝送形態を示す説明図である。

【図 8】

IEEE 1394 における Packet 送信の概要を示す説明図である。

【図 9】

上記データ伝送システムにおけるデータ送信装置の要部構成を示すブロック図である。

【図 10】

上記データ送信装置の動作を示すフローチャートである。

【図 11】

上記データ伝送システムにおけるデータ伝送の手順を示すフローチャートである。

【図 12】

上記データ伝送システムにおけるデータ送信装置側の処理手順を示すフローチャートである。

【図 13】

上記データ伝送システムにおけるデータ受信装置側の処理手順を示すフローチャートである。

【図 14】

上記データ伝送システムにおけるデータ伝送の他の手順を示すフローチャートである。

【図 15】

上記データ伝送システムにおけるデータ送信装置側の他の処理手順を示すフロ



ーチャートである。

【図 1 6】

上記データ伝送システムにおけるデータ受信装置側の他の処理手順を示すフローチャートである。

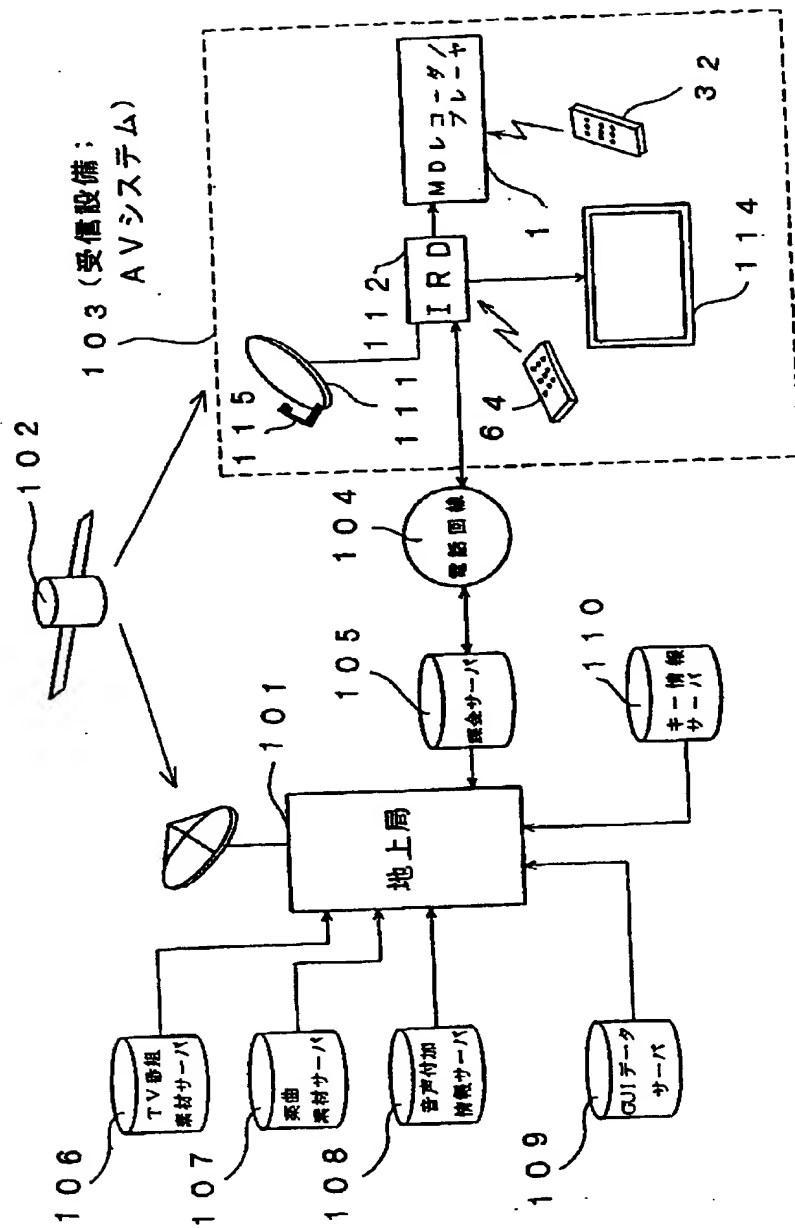
【符号の説明】

1 0 データ送信装置、2 0 データ受信装置、3 0 伝送路 3 0、1 1, 2  
1 内部バス、1 2, 2 2 CPU、1 3, 2 3 メモリ、1 4, 2 4 入力イ  
ンターフェース、1 5, 2 5 ユーザインターフェース、1 6 入出力インター  
フェース、1 8 衛星アンテナ、2 6 メディアアクセス部

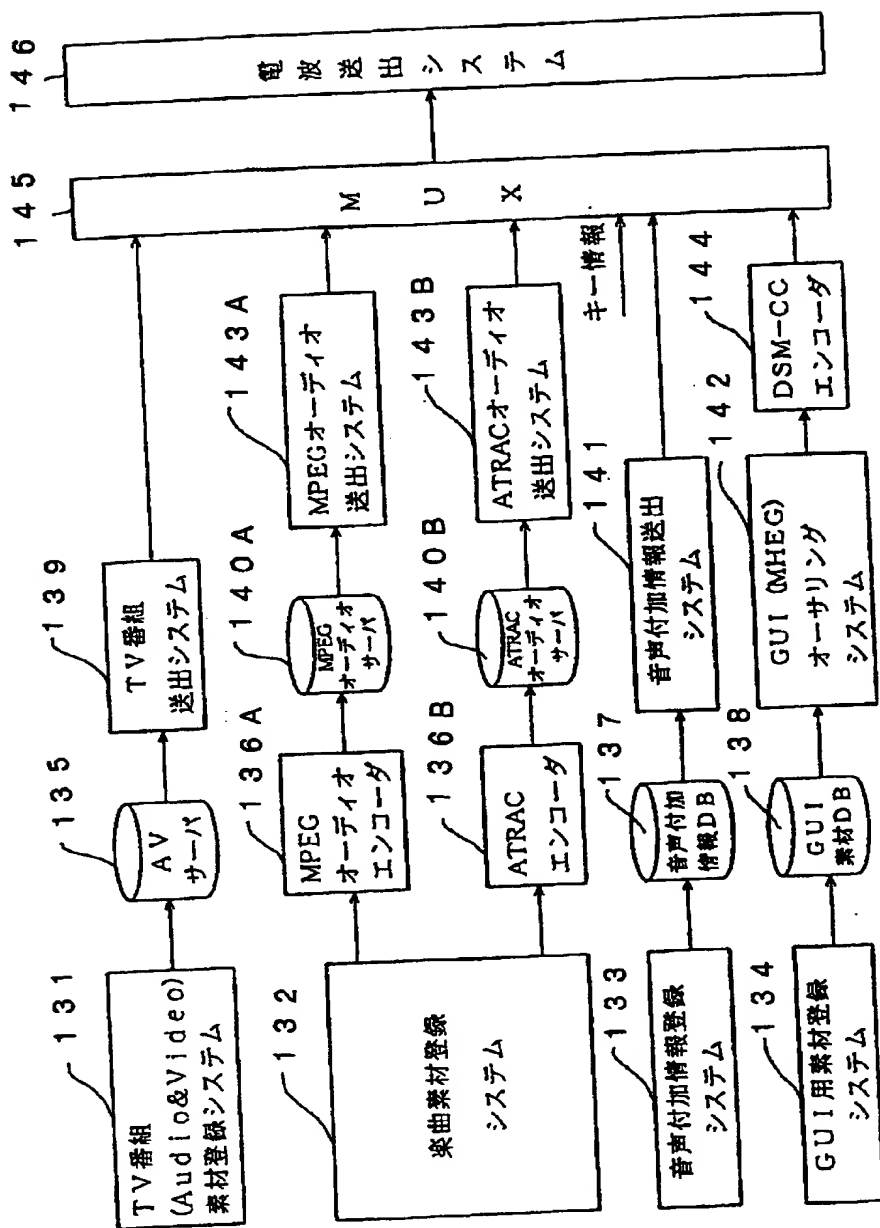
【書類名】

図面

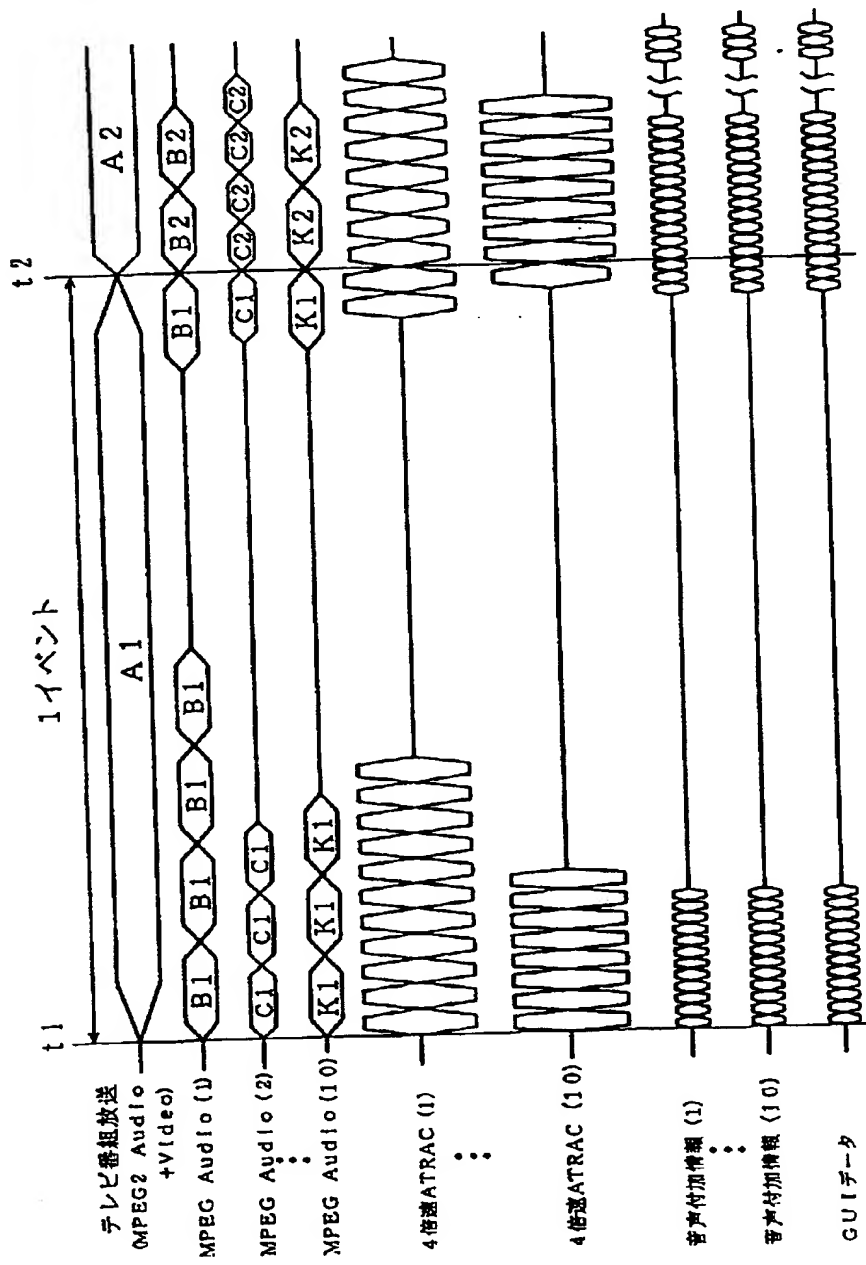
【図 1】



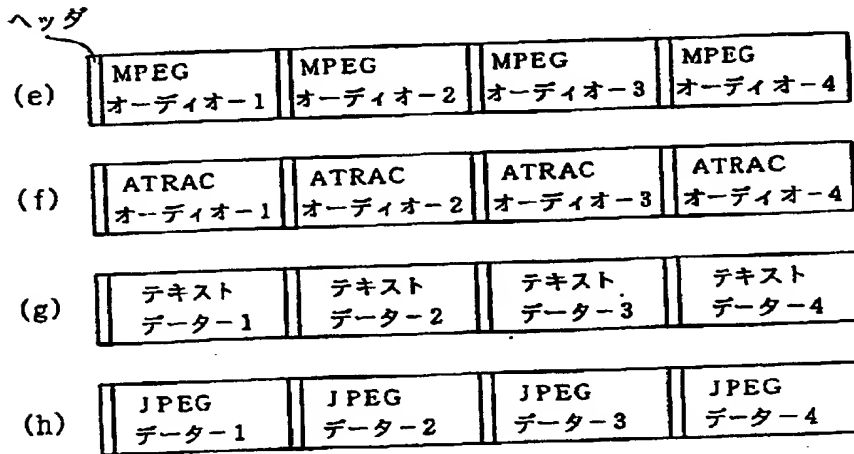
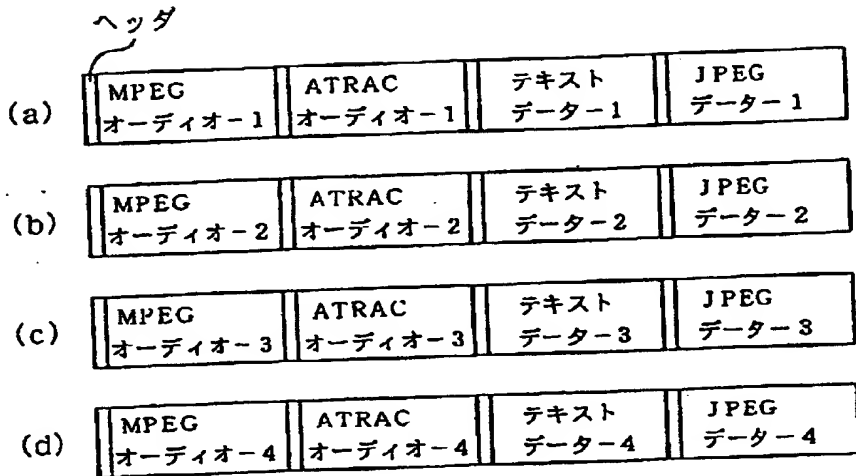
【図 2】



【図 3】

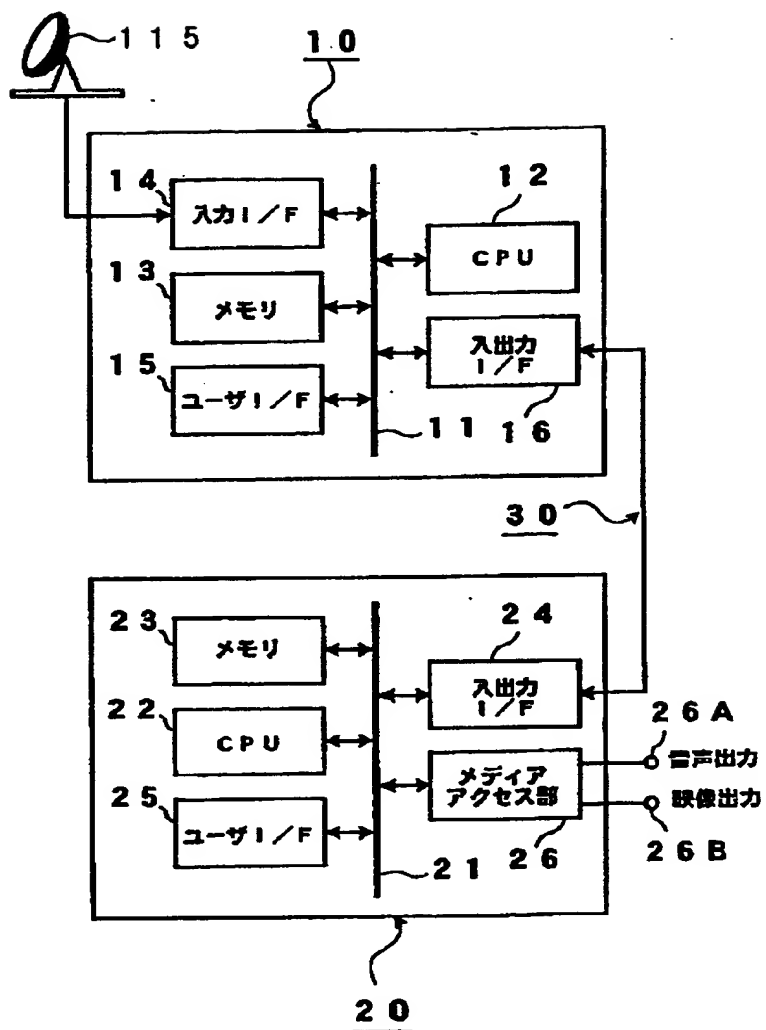


【図4】

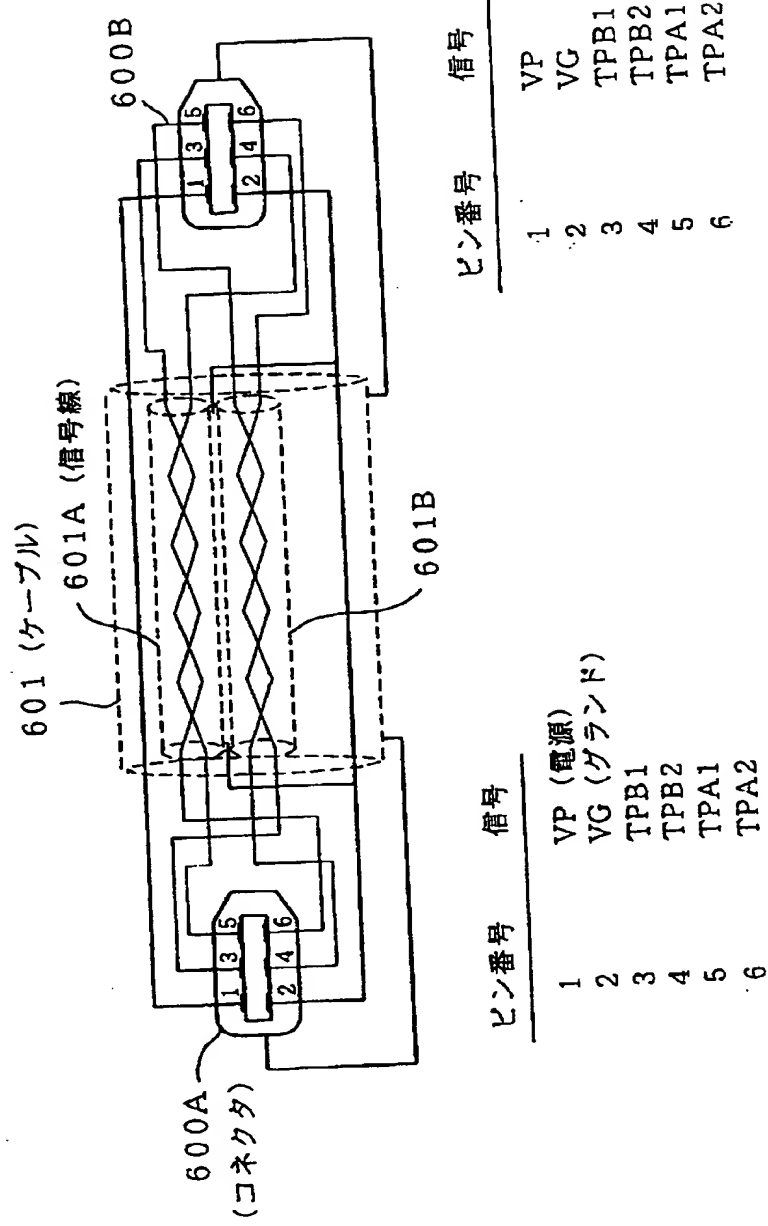


送信側の時分割多重化

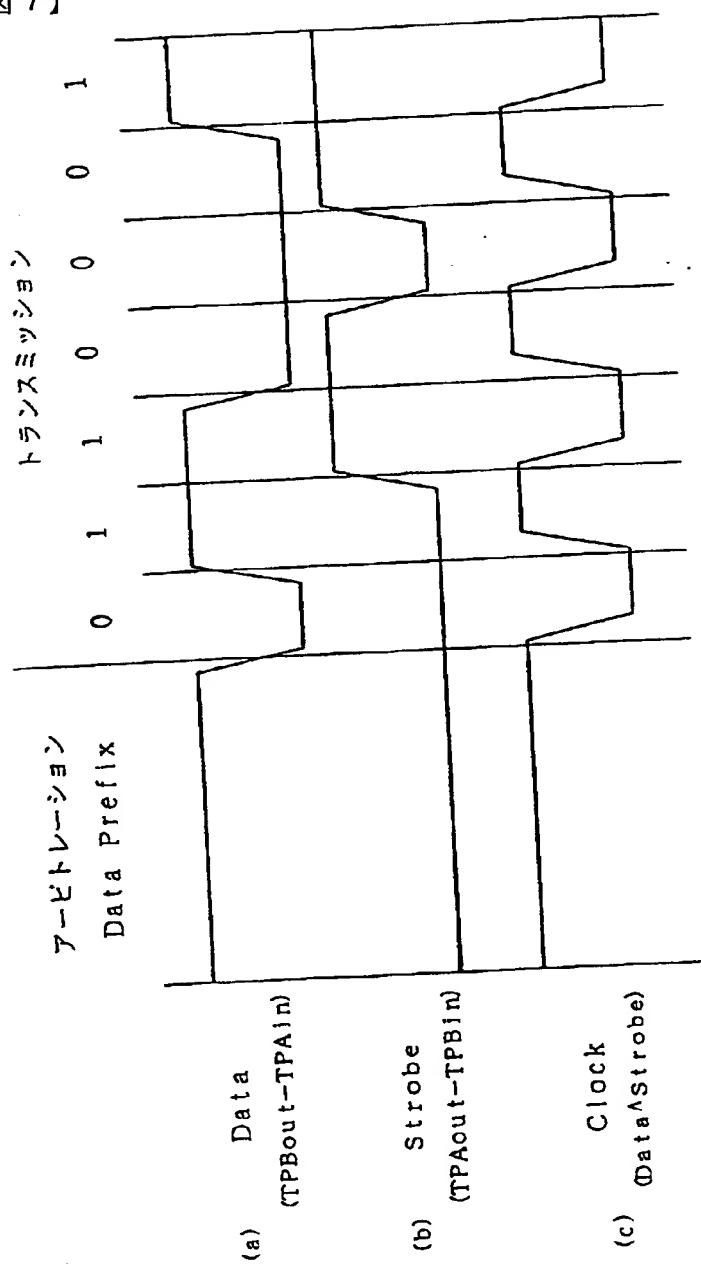
【図 5】



【図 6】

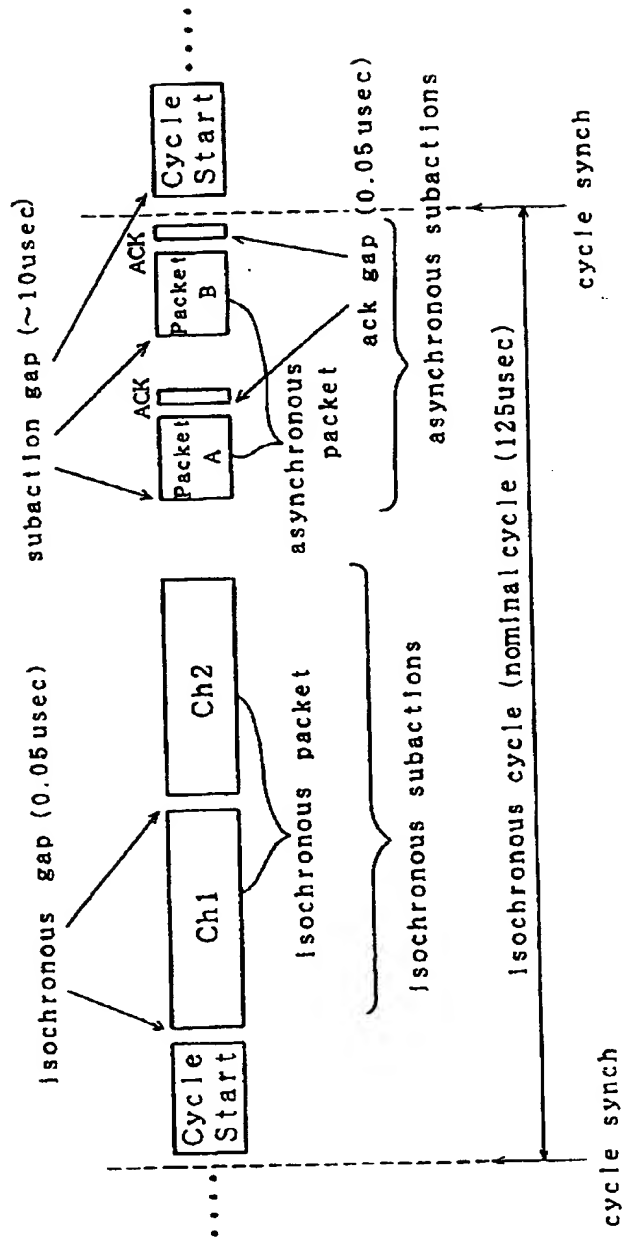


【図 7】

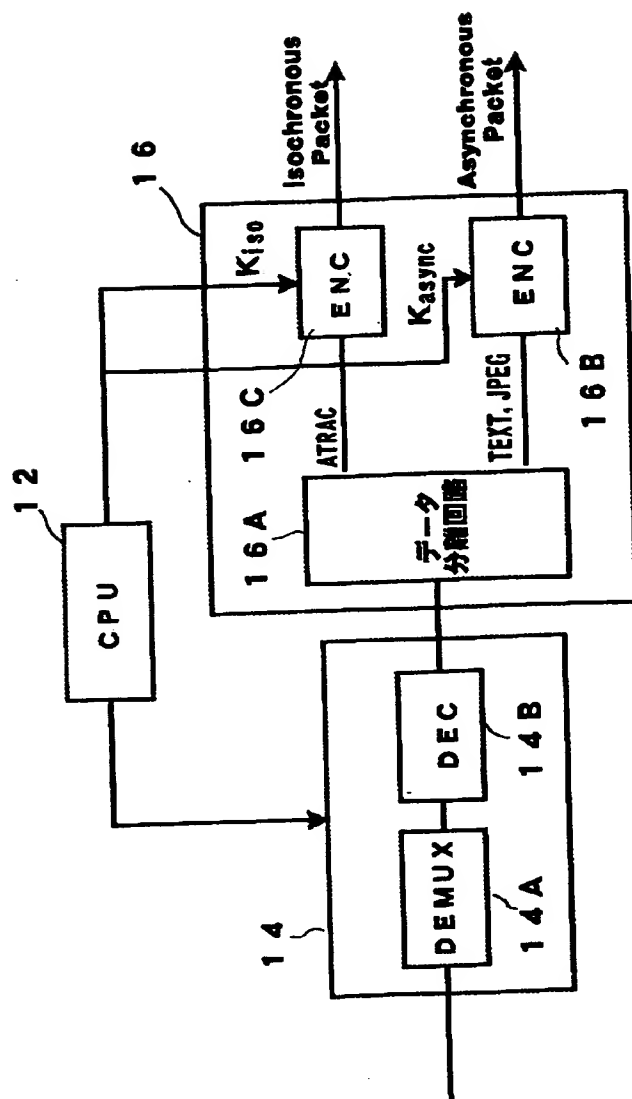




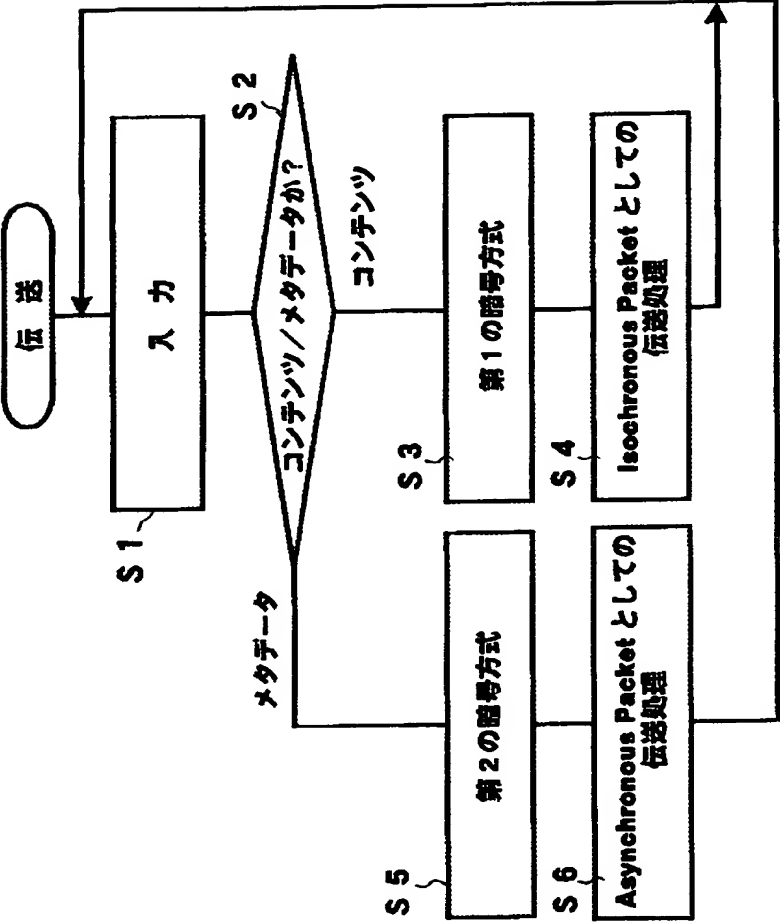
【図 8】



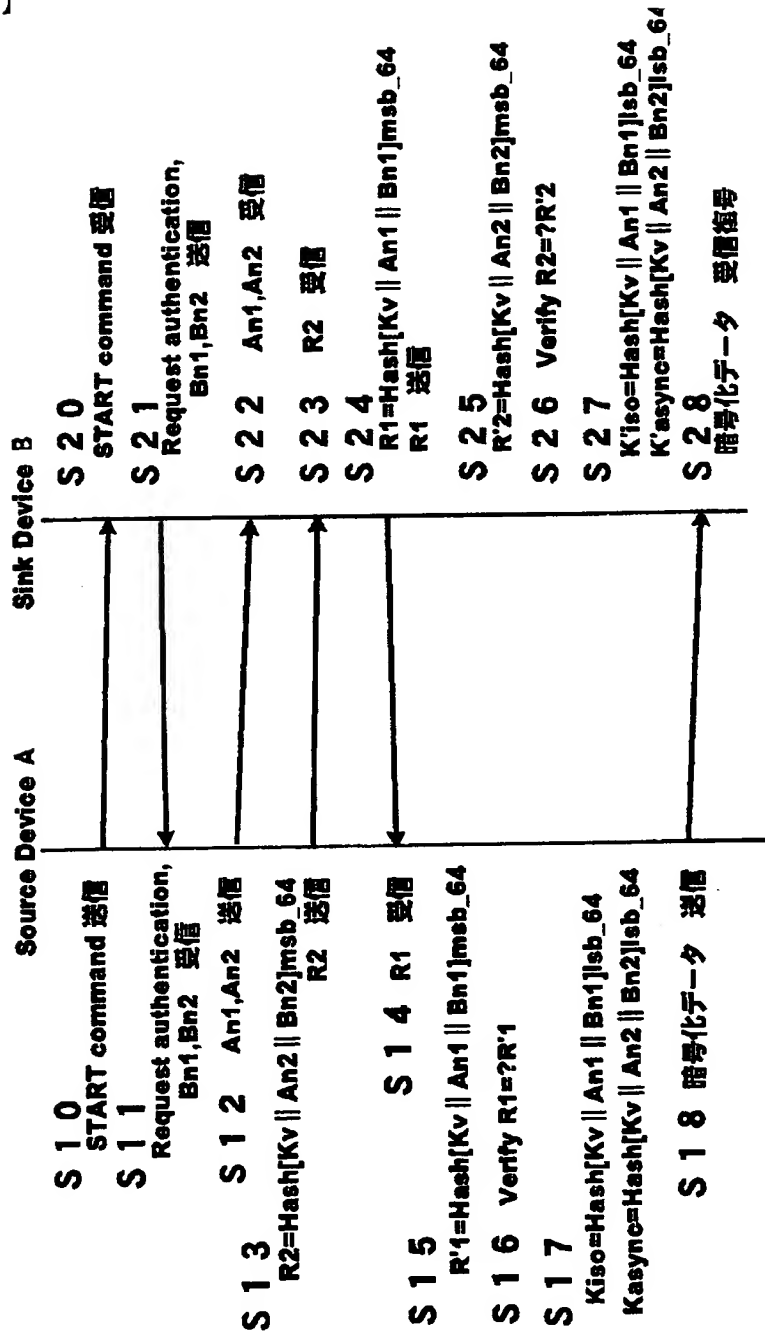
【図 9】



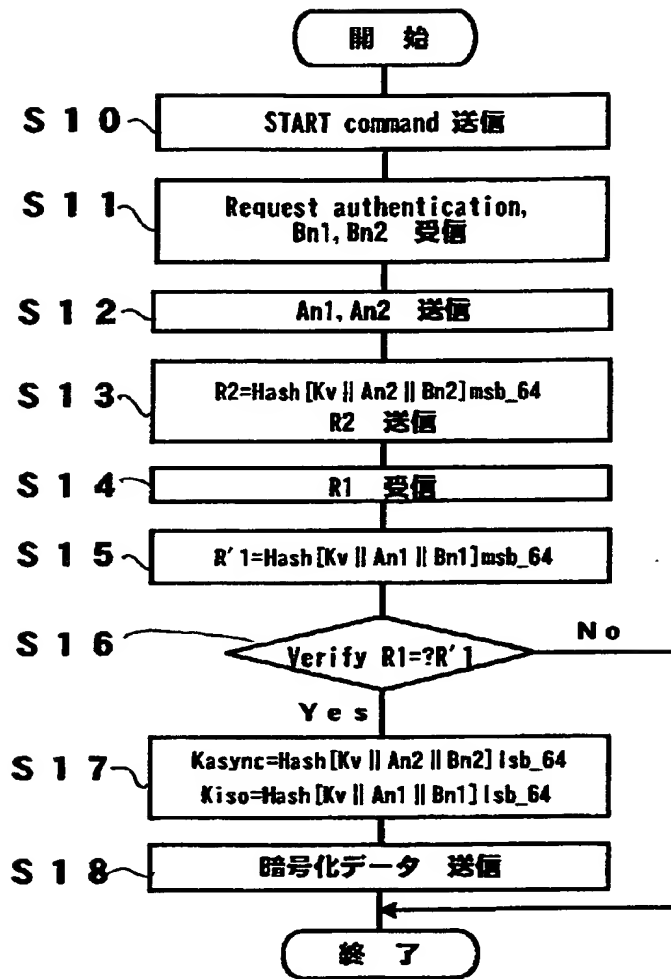
【図 1 0】



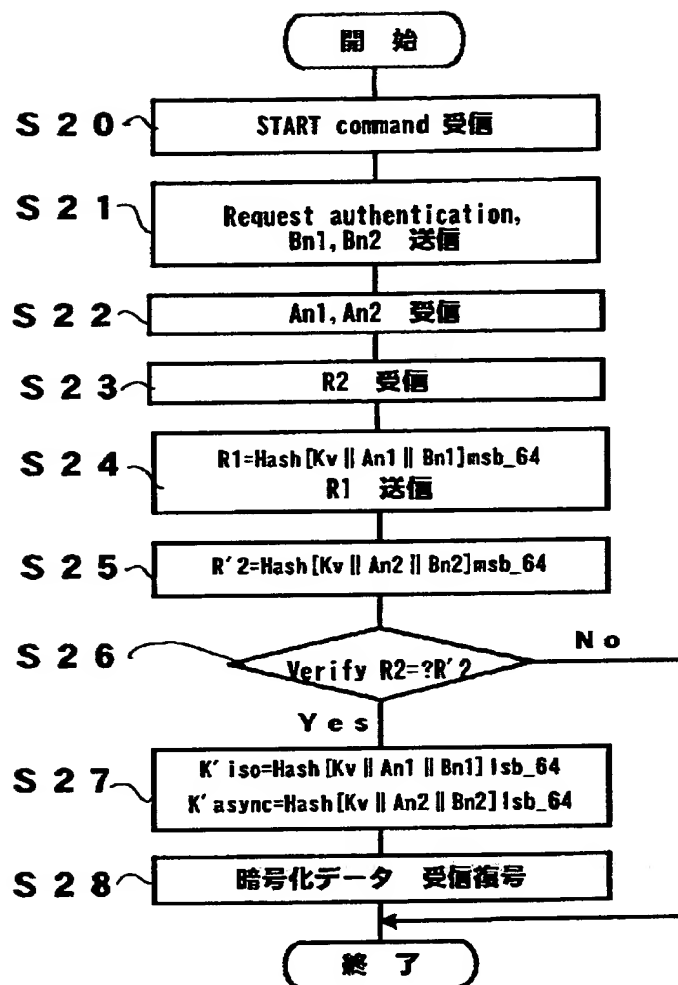
【図 1 1】



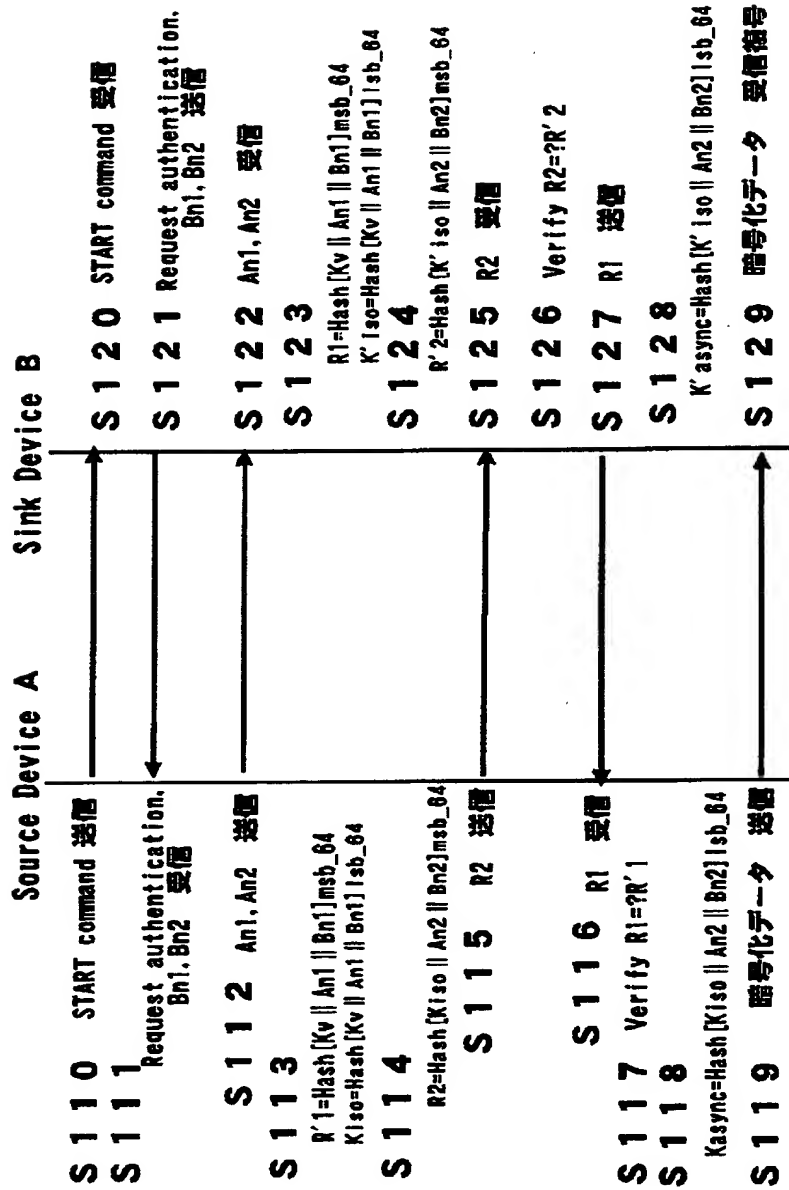
【図 12】



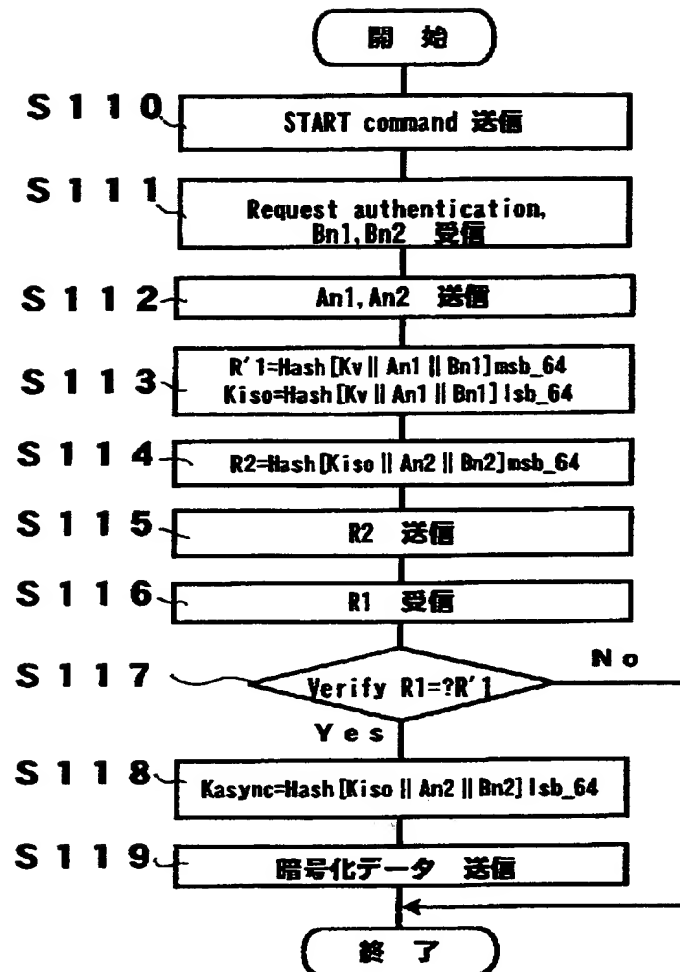
【図 1 3】



【図 1 4】

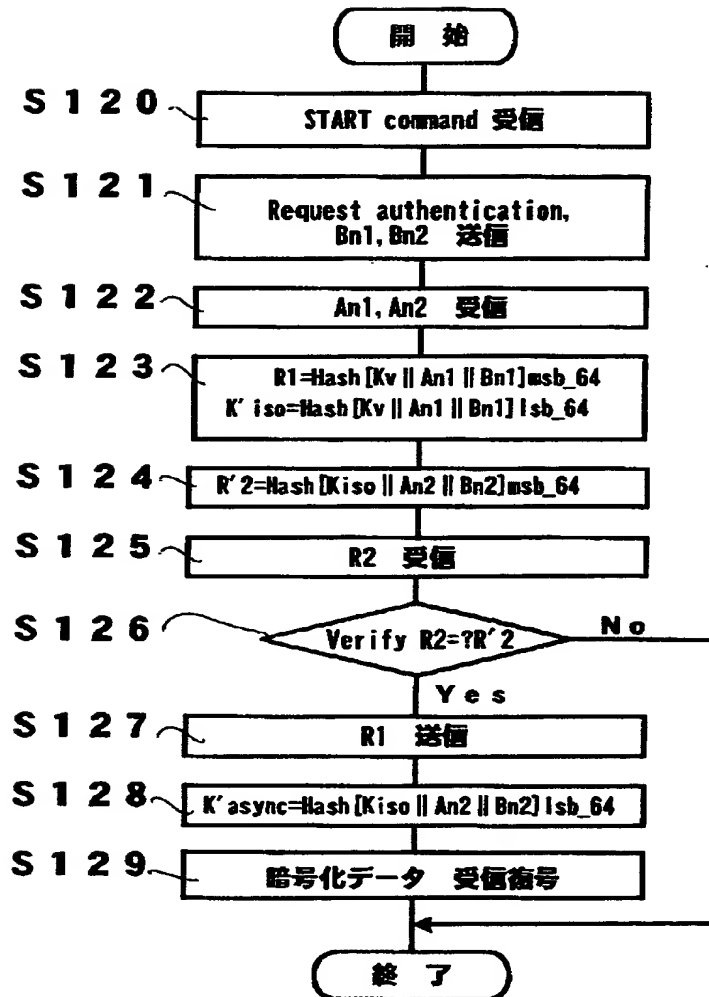


【図 1 5】





【図 1 6】



【書類名】 要約書

【要約】

【課題】 伝送帯域が確保された伝送方式と伝送帯域が確保されていない伝送方式の 2 種類の伝送方式を採用して、データを安全かつ確実に伝送する。

【解決手段】 データ送信装置 1 0 側の CPU 1 2 とデータ受信装置 2 0 側の CPU 2 2 と間で、データ伝送に先立って、相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する。データ送信装置 1 0 は、伝送帯域の保証が必要なデータを上記 CPU 1 2 により第 1 の暗号鍵で暗号化して第 1 の伝送モードで入出力インターフェース 1 4 を介して送信し、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで上記入出力インターフェース 1 4 を介して送信し、上記データ受信装置 2 0 は、上記 CPU 2 2 により、入出力インターフェース 2 4 を介して第 1 の伝送モードで受信される上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で復号し、上記入出力インターフェース 2 4 を介して第 2 の伝送モードで受信される上記関連データを第 2 の暗号鍵で復号する。

【選択図】 図 5

認定・付加情報

特許出願の番号	平成 11 年 特許願 第 143988 号
受付番号	59900488112
書類名	特許願
担当官	第八担当上席 0097
作成日	平成 11 年 5 月 28 日

<認定情報・付加情報>

【特許出願人】

【識別番号】 000002185

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 35 号

【氏名又は名称】 ソニー株式会社

【代理人】 申請人

【識別番号】 100067736

【住所又は居所】 東京都港区虎ノ門 2 - 6 - 4 第 11 森ビル 小池国際特許事務所

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【住所又は居所】 東京都港区虎ノ門 2 丁目 6 番 4 号 第 11 森ビル 小池国際特許事務所

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【住所又は居所】 東京都港区虎ノ門二丁目 6 番 4 号 第 11 森ビル 小池国際特許事務所

【氏名又は名称】 伊賀 誠司

次頁無

特平 11-143988

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社